IoT at the Edge

Succeed with IoT

IoT at the Edge:

Enabling the Real Time Enterprise

beecham research

Shaping the IoT future

Proud to sponsor this important report that seeks to improve the success rate of the Real Time Enterprise...

Contents

CLICK THE IMAGE TO GO STRAIGHT TO THAT SECTION

Introduction

IoT has moved away from the old model of processing all IoT data in the cloud, which limited its role to monitoring and reporting. Processing data at the edge enables local control and automation. IoT at the Edge will transform IoT in enterprise operations.

IoT at the Edge represents a step change in IoT and is reinforced by the introduction of 5G. In many ways, it is also consistent with the increasing interest in private networking which is also being significantly enhanced by 5G. The opportunities for 5G private networking are explored in the sister publication to this report, available via free download at: www.5GPrivateNetworking.com.

Both of these reports are part of Beecham's popular 'Succeed with IoT' series, which commenced with 'Why IoT Project Fail', available via free download at: www.whyiotprojectsfail.com. The second in the series is 'How to Succeed with IoT', also available via free download at: www.succeedwithiot.com.

This report combines Beecham's own research with publicly-available research from other named sources, together with insights from our sponsors. It is aimed at enterprise users of IoT, as well as IoT application, product and solution developers and is accompanied by a series of shorter reports and on-line video sessions. Keep an eye out of these if you are looking for more detail on the topic of IoT at the Edge and would like to discuss the topic further.

Beecham Research has been involved in IoT for over 20 years and we see this as a particularly important next step in the evolution of the IoT market and of IoT solutions to meet enterprise needs. This comes at a time when there has never been more choice for connecting devices to the Internet. Gone are the days when the choices came down to Wi-Fi in the local area and 2G cellular in the wide area. Now, it is increasingly important to select the most appropriate connectivity for the application need bearing in mind that the connectivity technologies are also continually evolving. It was once said that IoT connectivity will just become a lowest cost commodity. Now it is clear that was never the case and is highly unlikely to ever be the case. Without connectivity there is no IoT.

Likewise, the growing need for data must be accompanied by local intelligence to make the most of it. It was once said that the real future of IoT is data analytics in the cloud. Now it is abundantly clear that too is not going to be the case.

The aim of this report is to explore the wide range of opportunities for enterprise users that IoT at the Edge opens up. This is not a topic than can be ignored. As the market statistics in this report show, IoT at the Edge is inevitable for most IoT applications at some stage. As shown in Section 2, there are several application groups where it is already vital and this will grow as enterprises need to adopt more real-time methods of operation. In Section 3, we take a look at what people in the market are saying about IoT at the Edge and what that means in terms of market trends. In Section 4, we look at what is needed to deploy IoT at the Edge as part of IoT solutions.

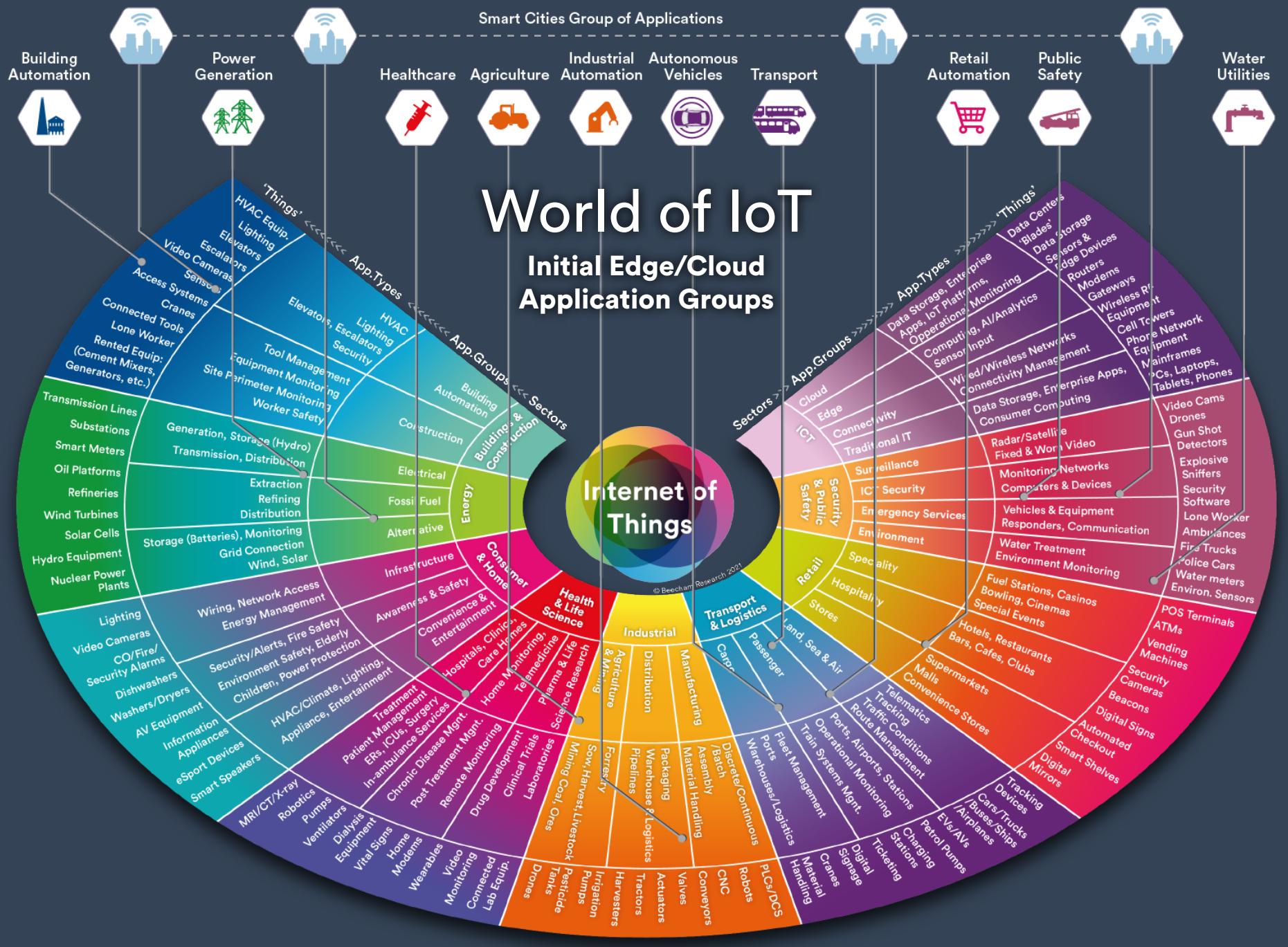
Is the market ready for IoT at the Edge? Not particularly. Does the market need it? Definitely. Does this represent a potential competitive advantage in their own markets for first-mover enterprises? Very likely.

This is intended to be a reference document for those responsible for IoT projects within their companies – users of IoT solutions – as well as those who develop and supply those solutions. We hope you find it useful.

Robin Duke-Woolley
CEO, Beecham Research

IoT Sector Activities

With many IoT applications moving to real time operation, where is IoT at the Edge currently having most business impact? What are the key influences? This section examines the main areas of IoT transformation now and in the near future. Use cases are shown with a dark background to highlight them.



Application Groups for Cloud-Edge Processing

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

The inner ring names the nine **Sectors** in question, from Buildings and 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 go down to greater detail naming actual applications serving a specific purpose, e.g. building site perimeter monitoring for construction, chronic disease management for healthcare.

Finally the **Things** are not applications but the end items which are instrumented and monitored through the named applications, e.g. glucose levels in patients' blood, readings of temperature and humidity in outhouses in farms.

The chart highlights application groups where significant edge processing is already taking place. One of these groups is Smart Cities which itself contains application groups from different sectors, making it an example of an application group overlay.

Edge processing is a relatively new addition to the Information and Communications toolset but opens up new possibilities gained from processing some of the IoT data locally rather than sending it all to the Cloud. The industry is expecting a significant increase of applications at the Edge in the next three years.

In the paragraphs below we examine the benefits of Edge processing as applied to IoT solutions in selected vertical markets. We expect that as Edge processing proves to open new possibilities, adoption will spread to many more applications in all IoT sectors.

Applications Enabled by Cloud-Edge Processing

Building Automation

- Space Optimisation
- Load Management
- Precautionary Maintenance
- Employee Services Requests
- Support Staff Resource Planning

Power Generation

- Forecasting Energy Demand
- Optimising Generation Efficiency
- Demand Management
- Enhancing maintenance tasks
- Unlocking Renewables.

Healthcare

- Remote Patient Monitoring
- Connected Inhalers
- Ingestible Sensors
- Surgical robots
- Drug Discovery

Industrial Automation

- Smart Factories & Warehouses
- Industrial Robots
- Wafer Handling
- Complex Machining
- Motion Control
- Machine Vision
- Industrial Safety

Agriculture

- Vertical Farming
- Predictive Analytics
- Crop & Soil Monitoring
- Drones
- Crop Planning.

Autonomous Vehicles

- Vehicle-to-Vehicle Comms
- Vehicle-to-Everything Comms
- In-Vehicle Safety
- Road Safety
- Emissions Reduction

Transport

- AI Data Driven Applications
- People Centric Applications
- Intelligent System Simulation

Retail Automation

- Personalised Content Delivery
- Optimise Staffing Levels
- Automated Payment Systems
- Movement Tracking
- Warehouse Robots
- Wireless Shipment Tracking
- Real-Time Condition Monitoring
- Inventory Management

Public Safety

- Preventative Policing
- Criminal investigations
- Number Plate Recognition
- Background Checks
- Real-Time Location Sharing
- Disaster Notification

Water Utilities

- Improving Distribution
- Demand Management
- Enhancing Maintenance
- Customer Experience

Smart Cities

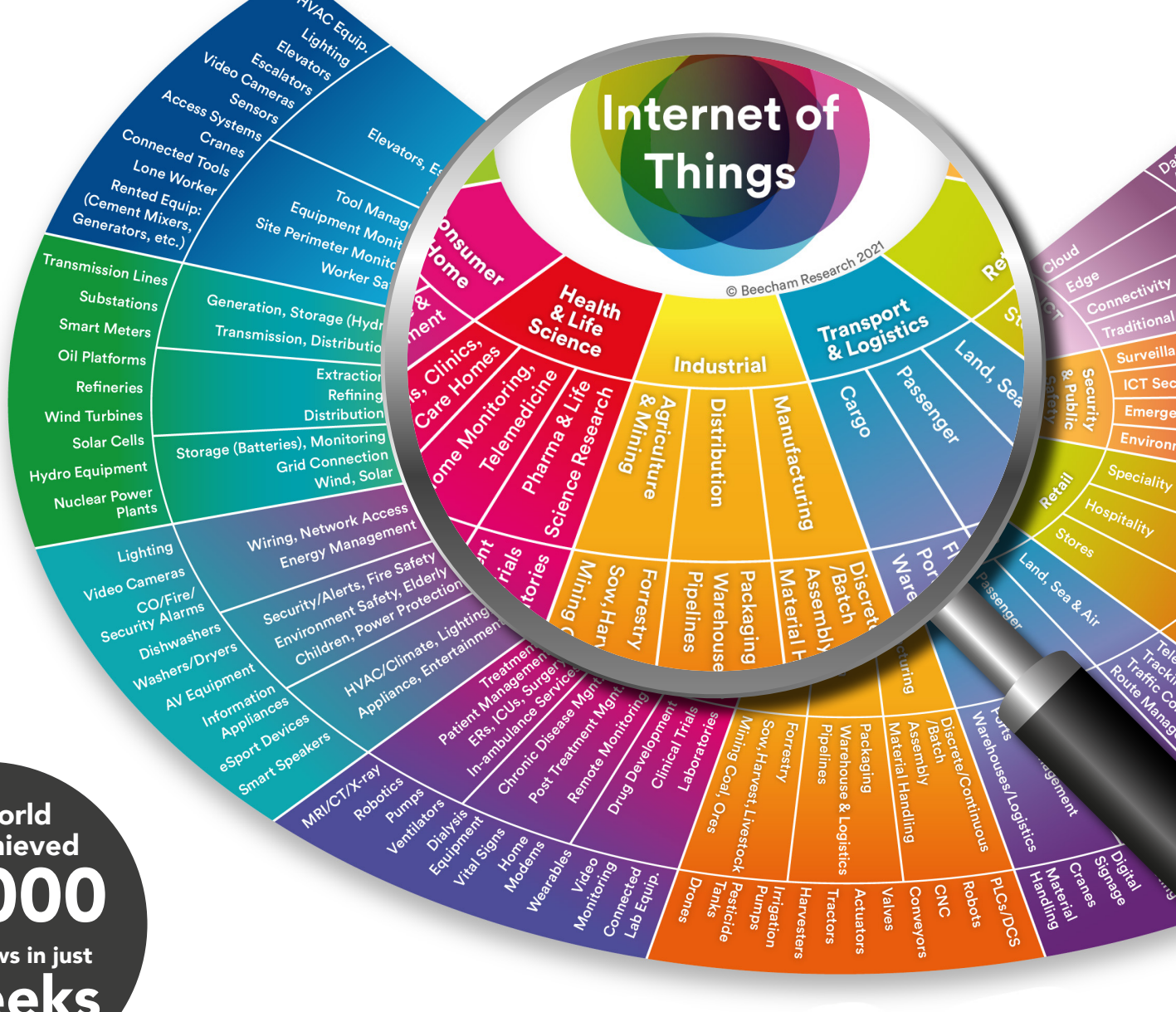
- Traffic Management
- Rail & Bus Coordination
- Taxi Regulation
- Parking
- Highway Maintenance
- Traffic lights, Signage, Lighting
- Emergency Response
- Environmental Monitoring
- Water Monitoring & Maintenance
- Trash Disposal
- Disaster Notification
- Video Surveillance
- Energy management
- Social Distancing
- Building Maintenance

CLICK THE ICON TO GO STRAIGHT TO THAT APPLICATION

THE IoT WORLD MAP

Put your IoT Business on the Map!

List your sales rep, product, service & case study to get in front of 350K potential IoT buyers



IoT World Map achieved 50,000 unique views in just 4 weeks

www.iot-now.com/world-of-iot

Become a Map Member

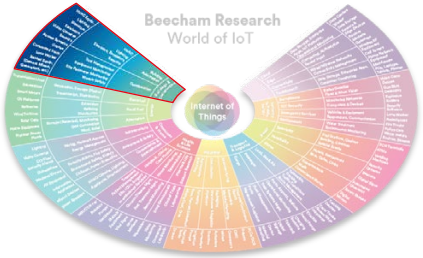
Get 12 months of unparalleled industry exposure

Contact **Emma Collins** today on **e.collins@wkm-global.com**

IoTNOW
HOW TO RUN AN IoT ENABLED BUSINESS

In association with beecham research

Building Automation



The challenges

Building automation refers to the centralised control of a building's HVAC, electrical, lighting, shading, access control, security systems, and other interrelated systems. Advanced, cost-effective IoT devices and pervasive wireless connectivity provide huge amounts of meaningful data on the building's infrastructure (climate, water and energy usage) as well as room occupancy and occupant behaviour during the course of the day.

Platforms running on Edge gateways and/or servers onboard aggregate and normalise data from the many different IoT sensors and Edge devices, making it available for Edge decision making, AI analytics and automatic control. The data or a subset can also be streamed to a cloud or an in-house data facility to run detailed data processing such as trend analysis.

The new dimension that AI brings to the building automation environment is the use of autonomous analysis of the data as a basis for optimised operation. For example, the heating and cooling dynamic of rooms and weather forecasts can be incorporated. Cleaning schedules can be based on the predicated use of kitchens, canteens and toilets as well as earlier usage patterns. Similar benefits can be obtained from other service areas.

The combination of intelligent Edge computing and AI analytics makes buildings 'smart' – i.e. buildings that help managers streamline and optimise operations while minimising the impact on the environment. These and other business benefits are all predicated on the intelligent evaluation of baseline building data.

Applications

Optimised utilisation of spaces and infrastructure: capacity analysis and forecasting, e.g. for meeting rooms, canteens, pantries, transit areas, toilets and parking spaces

Load management: forward-looking operation of electrical systems in order to avoid (costly) peak loads.

Precautionary maintenance and optimised servicing: analysis of failure probability, timely maintenance and avoidance of technical failures.

Employee-oriented value-added services: mobile devices can request parking space availability and preferred workspace location

Compensate skilled-staff shortages: enable maintenance staff to manage the building's technical systems.

Building Automation

Case Study – Smart Buildings

The company partnered with Sierra Wireless to create a monitoring unit based on Sierra's HL7800 module. These units can be installed alongside existing HVAC systems to provide remote monitoring and predictive maintenance. The HL7800 module collects critical data-points from sensors within the HVAC and sends it back to the cloud via a cellular connection.

As a result, the company can now provide its customers a touchless maintenance experience. Service personnel can monitor a customer's HVAC remotely and send them a report once a year. If the equipment is working well then there is no need for a physical site visit, saving unnecessary expense. If there are issues than a service team can come and fix the equipment. Importantly, they will already know what the fault is, meaning they can arrive with the correct parts, reducing time spent and increasing the first-time-fix rate.

The HL7800 module uses a LTE Cat-M1 standard. This is a fast, low-power system that works well for HVAC equipment because it has very good reach and propagation. Residential HVAC systems can be located in houses in rural locations with poor cellular coverage. Also, the metal of the HVAC system itself can also cause interference. LTE Cat-M1 provides very reliable connectivity for IoT devices, even if they are obstructed or located in basements, or are in remote locations. Also, because power consumption is so low, the HL7800 can operate for years without the battery needing to be replaced.

In addition, the company used Sierra Wireless' Enhanced Carrier Connectivity (ECC) solution. ECC is designed to optimize IoT connectivity in North America (NAM). It utilizes Sierra's Global Network Operating Center (GNOC) to constantly track cellular networks through North America to ensure they are running smoothly with no disruptions. Sierra has direct lines to all of the major carriers in NAM, so if there is a network outage, we can quickly trouble-shoot the issue and get it resolved. With ECC, all the IoT devices in the network can be organized and monitored through Sierra's cloud-based management platform.

Benefits

- The HL7800 has enabled the company to save costs and provide a better customer ex-perience, through moving to a precision, predictive maintenance system for its HVAC systems. Due to its versatility and interoperability, the HL7800 is able to synch easily with many different types of HVAC equipment, not just those made by the company.
- The company has been able to divert resources away from servicing HVAC equipment to more profit-generating activities like installing new systems.
- The module's low cost and robust connectivity has made it perfect for large-scale de-ployments and residential equipment. Predictive maintenance only works with a reliable connection. No connectivity – no data. The HL7800 runs on the optimal CAT-M1 standard and is supported by Sierra's ECC solution, which further maximizes uptime and availability.

Building Automation

psacertified™

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.

Embedded Planet

Building Automation

psacertified™

Case Study – Construction

Data is becoming as fundamental to the construction industry as bricks or mortar. If companies have access to real-time information on their assets they can monitor, analyze, and optimize their performance. An increasing number of Internet of Things (IoT) devices are being deployed to provide that intelligence, but they can also expose firms to risks as not all these connected products have been designed with security in mind. With a growing risk of cyberattack, connected products must have security built in.

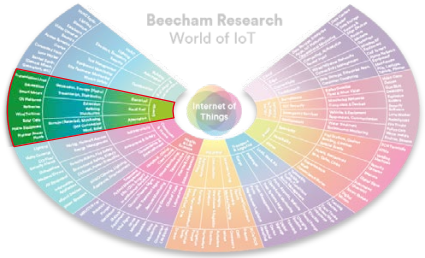
To help industries benefit from IoT innovation without becoming an easy target for hackers, global technology, supply chain, and manufacturing solutions company, Flex, developed its iENBL low power, rapid development platform, using the ST Microelectronics STM32L4 (Arm Cortex-M4). Start-ups are using the platform to reduce the time and cost involved in developing and testing IoT devices that solve the construction sector's challenges. MachineMax, for example, is a UK-based company that wanted to help customers track and manage their heavy machinery. It had realized that, in some cases, its customers' off highway vehicles were idling up to 50% of the time, at a cost of tens of thousands of dollars.

Flex helped MachineMax speed up the development of an IoT tracker that can improve the efficiency of a fleet, reduce maintenance and environmental costs, and increase productivity on site. Importantly for MachineMax and its customers, who need to be able to trust the device and the data it generates, Flex had built security into its platform from the outset.

Deploying security features into connected devices is tricky, so Flex used the PSA Certified security framework to help assure customers that their product is protected against the most common cyberattacks. Flex took proactive steps to achieve PSA Certified Level 1 certification, on their iENBL platform, which means its security is in line with industry best practice and meets major cybersecurity standards, requirements, and regulations.

flex

Power Generation



The challenges

IIoT is being implemented in this sector to optimise energy generation as well as distribution to help providers keep up with the increasing demand for gas and electricity. Smart meters provide near real-time information on consumption, which enables more efficient, demand-based electricity generation and distribution.

Artificial Intelligence's ability to generate prediction information is enabling better demand forecasting; predictions can now go far beyond the weather, for example, how much additional power is used during a festive event. AI can perform these complex tasks at speed and enable decisions to be automated and made in real time.

AI can also improve regular energy storage technology by making it easier to integrate different technologies, e.g., renewable-powered microgrids and utility-scale battery storage. The role of energy storage in modern grids is growing rapidly along with the proliferation of intermittent power sources like wind and solar.

Edge computing, in which data is processed locally near the source, saves processing time and reduces the need for Internet access. It is being adopted by utilities and energy companies whose assets are widely distributed.

Global energy demand is set to double by 2050. However, legislation requires utilities to find ways to reduce carbon dioxide emissions, lower energy consumption and introduce alternative fuels. Driving operational efficiency is also a top priority. This combination represents a very big challenge, one that another combination, that of IoT, Edge computing and AI helps address.

Applications

Forecasting energy demand

Optimising power generation efficiency

Supporting demand management

Enhancing maintenance tasks

Unlocking the vast potential of renewables.

Power Generation

Kigen

Case Study – Pioneering Customer Centric Services for Smart Grid with eSIM Enabled Metering

Challenge: Global smart metering solutions provider Iskraemeco helps energy companies effortlessly deliver customer insights and functionality. To serve the global shift to a more resilient, reliable smart grid, it needed a flexible and simplified route to market for smart meters destined for multiple markets across the world.

For it's utility customers to unlock the potential of data insights and intelligence, these edge devices need to meet strongest standards of security and serve long in-field service lifespans withstanding local specification changes. Robust security 'built for IoT devices' and enabled on ultra-low power connectivity were key to Iskraemeco's innovation team for the design of their modular fourth generation smart meters.

Solution: Iskraemeco's team foresaw new possibilities in how data can generate revenue streams for utility providers, positioning them as broader service providers. That's why Iskraemeco transitioned to an eSIM with Kigen OS software, created and supplied by Workz. Each eSIM comes personalized with a global bootstrap, enabling both factory over-the-air meter testing and out-of-the-box global connectivity from Kigen's ecosystem of partners. If a local network is preferred, the Kigen remote SIM provisioning (RSP) service can provide a local operator profile with no need for physical access to the device. Interoperability across MNO profiles as well as modular subsystems remove hurdles for utilities when integrating mobile technology for large-scale, cost-sensitive smart meter deployments. Further ease of Kigen's RSP server's application programme interface (API) brought a unified workflow for companies, a big step towards easier adoption across the smart grid ecosystem.

New Possibilities – Smart Meters as Edge Devices: Edge processing can help to manage and extract more value from the data in the age of growing grid management complexity. Meters will have more edge computing capability in the future," says Gregor Rodi, innovation manager for connectivity at Iskraemeco, "Smart meters will process the data where the data is collected, at the edge, pick the insights needing cloud processing and empower local corrective action, enabling more grid flexibility. Integrating security technology opens (these) new possibilities"

By utilising smart metering and other technologies, utility providers can start providing value-added services such as dynamic pricing, real-time billing, and real-time access to connected devices for remote analysis and maintenance, and usage control. New services open new revenue streams for utility providers, positioning them as broader service providers. Smart meters can become hubs for interoperating with all sorts of IoT devices and sensors at customer locations.

Result: Iskraemeco's meter trials enabled by Kigen's eSIM technology have been successful across multiple countries with multiple utilities in each. A choice of MNOs in regional deployments offered through Kigen's RSP service prevents lock-in for utility customers and alleviates concerns over varying signal quality in some areas.

Wider applicability: eSIM technology is ready for smart metering, and many other IoT Edge use cases. Enterprises can take advantage of eSIM and it's integrated form factor – iSIM, and the broad cellular IoT coverage to serve more markets and customer requirements with ease, get better insights and – ultimately - gain competitive edge. This clear market opportunity presents an attractive opportunity for enterprises to capitalise on serving customer centric services such as usage tailored pricing, insurance-based incentives, and billing and more!

Power Generation

Case Study – Large Wind Turbine Manufacturer

A leader in manufacturing wind turbines, this customer uses Cumulocity IoT both on-premises and at the edge, as well as Software AG's streaming analytics capabilities to autonomously manage clean-energy wind farms based on sensor data.

Challenges

- Reduce the cost of energy from newly installed wind turbines
- Develop turbines of even greater efficiency
- Optimize the total lifecycle costs of operating and managing the whole wind power delivery
- Replace SCADA-based approach with an integrated, IIoT platform-based windfarm control center

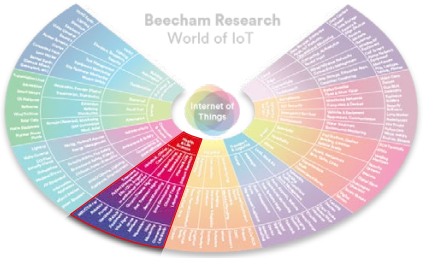
Solution

- Cumulocity IoT powers the integrated wind farm control center, automating operations using real-time wind turbine data at the edge feeding back to the cloud
- 9,000+ wind turbines already connected throughout 30 countries
- 3,000 sensors per wind turbine
- > 25k data points ingested per second, 25 terabytes of stored data
- Management at local wind turbine as well as farm-level with the same software architecture from edge-to-cloud, i.e., identical APIs, data models, and analytics irrespective of the individual asset.

Business outcomes

- Projected 7% reduction in cost of energy (CoE) through improvement of operations efficiency by real-time analytics of wind farms and wind turbine generators
- Able to connect 500 legacy turbines a week during initial phase
- NEW service offerings incl. Condition Monitoring and Remote Monitoring
- 99.9% availability
- Decreased maintenance costs & improved predictability
- Use of latest wind turbine generator capabilities to increase OEE, development & deployment efficiencies through use of a single global software architecture from edge to cloud

Healthcare



The challenges

Healthcare systems typically comprise diverse silos of different IoT medical devices and applications, an infrastructure that increases costs and may constrain patient outcomes. Integrating those systems used to represent a challenge, but Edge computing uses a distributed computing model that enables the seamless integration of AI into healthcare ecosystems.

This development is delivering numerous benefits. For example, AI is being used to analyse big patient data sets, which provides patient insights and predictive outcomes; this in turn helps the ecosystem discover key areas of patient care that require improvement. Moreover the time saved and the conditions diagnosed are key in an industry where the time taken and the decisions made can be life-altering for patients.

AI can also automate administrative tasks, like pre-authorising insurance and maintaining patient records. Before the development of electronic health records hospitals had multiple systems that handled different functions.

Edge computing works as a complement to the cloud, allowing decision-makers to choose where to best placed workloads. This strategy can help health systems optimise the collection, storage, and analysis of data, which for the average hospital can reach 50 petabytes each year. Telehealth is an established application that allows the elderly to maintain their independence while still getting the assistance they might need in an emergency. These have been particularly valuable in the context of the Covid-19 pandemic, which has prevented family members from visiting and helping elderly relatives. IoT devices can automatically collect health metrics like heart rate, blood pressure, temperature, and more from patients in their home environment.

Applications

Remote patient monitoring

Depression and mood monitoring

Parkinson's disease monitoring

Connected inhalers

Ingestible sensors

Drug discovery.

Healthcare

SIERRA WIRELESS

Case Study – Connected Medical Devices

The Challenge
The device provides an innovative approach to cancer therapy that is transforming patient's lives. However, as the company looks to expand around the world, it has a number of IoT challenges to overcome in order to optimize the performance of its equipment and maximize patient benefits.
The device requires secure and stable connectivity layer to ensure there is no break in the transmission of data to back-end systems.

Simplifying Global Connectivity
As the company expands its geographic footprint, connectivity is becoming more complex. Different countries have their own network providers and pricing plans. Managing multiple SIMs across a range of territories is both challenging and a drain on resources – Europe alone has hundreds of separate operators. When it comes to global deployment, there can also be issues with reliability, due to localized network disruptions or coverage gaps. These may require local troubleshooting in order to get back online, which can be costly and difficult to organize. The company wanted a simple way to connect its devices anywhere in the world, with a single platform to manage them all.

Data Security
Finally, patient data is sensitive and confidential and the company needed an IoT solution that ensured the highest standards of security. Cellular connectivity is both highly secure and data is encrypted by default which helps provide an extra layer of protection.

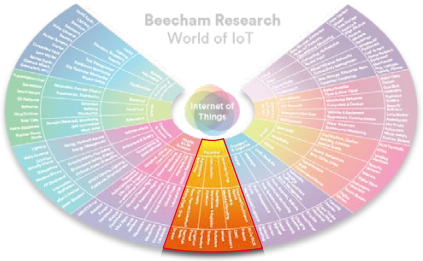
Overcoming The Challenges
By leveraging Smart Connectivity by Sierra Wireless, the company was able to build a reliable, easy-to-manage global solution for its products.

Connect Devices Globally with Smart Connectivity
Smart Connectivity solution includes a single global SIM that securely connects to cellular networks in 190+ countries. This has made it easier for the company to deploy its devices around the world as it only has one SIM vendor to manage.

Sierra's Core Network Maximizes Up-Time
The Smart Connectivity solution also provides an extremely resilient connection wherever the devices are deployed. Sierra Wireless's Core Network maintains secure access to multiple networks in each country. As a result, we are able to eliminate local coverage gaps. Sierra also maintains direct lines to all of the major network operators around the world, so if there is an outage, we can pro-actively troubleshoot the situation, this has taken the burden and cost of local management away from the company.

End-To-End Security
All of Sierra's solutions are built from the ground-up with security in mind. Our e-SIMs are designed to be concealed so as to prevent tampering or theft. We also have SSL encryption in our SIMs and at our multiple points of presence (POPs), which combines with encryption capabilities in the cloud to provide end-to-end integrated protection for sensitive data.

Industrial Automation



The challenges

The term 'Industrial Automation and Control' encompasses a comprehensive range of IoT activities that are related to data acquisition, monitoring, process control, analytics, modelling, simulation and process optimisation. Like Industry 4.0, this broad-based sector is making smart machines smarter, factories more efficient, processes less wasteful, and production lines more flexible. It builds on the foundation of smart, secure, wireless connectivity.

Industrial control systems are used to facilitate the integration of the devices, machines, and equipment within manufacturing plants. Industrial automation systems require tight integration between devices on the plant floor, the OT domain, and the rest of the enterprise, the IT domain. In turn it relies on the deployment of smart devices at the Edge for efficient data collection, and the ability to turn data into real-time actionable information.

The transition from Industrial Automation and Control to Industry 4.0 will depend on a successful adoption of many new technologies. For example, to accelerate smart manufacturing, digital twins of machines and operations will be employed as will real-time control of equipment and tasks.

A longer-term goal is the realisation of fully automated factories. This concept is based on an open system architecture that enables the seamless interaction of all automation components and higher-level systems. Realising this concept will be ensured by consistent data management, worldwide standards and uniform interfaces that go from the field level to the corporate management level.

Applications

Smart factories and warehouses

Industrial robots and 'cobots' (collaborative robots)

Medical and surgical robots

Wafer handling in the semiconductor industry

Complex machining; using CNC (Computer Numerical Control)

Motion control

Machine vision

Industrial safety

Industrial Automation

psacertified™

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.

EUROTECH

Industrial Automation

Case Study – Dürr

Dürr makes and services advanced robotic paint stations used by major vehicle manufacturers. To avoid costly errors during painting, Dürr wanted to monitor, gather and process real-time data on rotation speed and air supply at the paint stations. It was critical that this could be done autonomously at the edge without being dependent on communications with the cloud which meant aggregating and analyzing the data locally without having to send it to the cloud.

Solution

Dürr leveraged Cumulocity IoT to develop a software tool that seamlessly records all data from the automotive painting process. This creates a "digital fingerprint" for each painted body. If a quality problem occurs, the root cause can be determined immediately using the recorded data.

Business outcomes

- Reduced errors, thanks to real-time signals every 8 milliseconds
- Lower manufacturing costs from reduced rework
- Accurate, faster decision-making
- Ease of use allows operators to manage analytics and create automated rules on the fly
- Won the German Innovation Award 2020 with EcoPaintJet, a groundbreaking innovation for the highly selective painting of cars

Software AG call this "Democratizing IoT". In other words, Software AG enables field teams, like machine operators, process engineers and plant managers, to maximize their benefits from IIoT through the exploitation of their domain knowledge using Cumulocity IoT's self-service analytics and integrations. Dürr uses Cumulocity IoT Analytics Builder to define and process the anomaly detection rules for its robotic paint shops deployed at BMW, Volkswagen, Mercedes and other plants around the world.

Industrial Automation

Case Study – SMC

A global leader in the manufacturing of pneumatic equipment. SMC decided to extend its product lines with smart networking and decentralized intelligence using IoT, however there was a problem: While sensors in SMC components could detect the data, they had no way of enabling customers to visualize, analyze and act on it.

Challenges

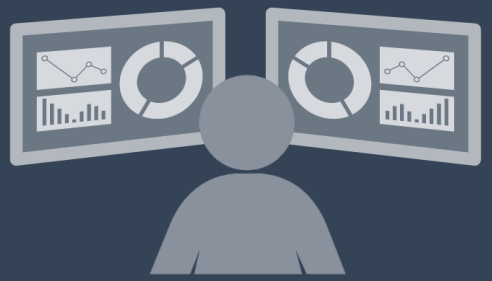
- Bridging the gap between data detection and data capture
- Growing customer demand for innovative ideas
- Need for an international expert that understands the requirements of all regions
- Genuine desire to see Industry 4.0 in factories
- Pressure to deploy an IoT-driven solution fast

Solution

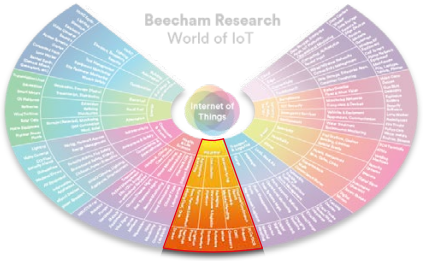
- Intelligent maintenance: Real-time cloud and edge-based visualization and analytics for machine monitoring & predictive maintenance
- Optimized operations: Forecasting combined with anomaly detection to identify process optimizations and increase overall equipment effectiveness (OEE)
- Increased energy efficiency: Optimized compressed air consumption enabled by real-time analytics of connected pressure and flow sensor data
- Identical components & tooling from edge to cloud with identical APIs, data modeling and analytics

Business Outcomes

- Solution rolled out in less than one week
- “Start small, scale fast” starting with just five to 10 sensors
- SMC’s new “Smart field analytics” solution available in under 4 months, providing a powerful, simple but easily scalable solution to customers
- With simple dashboards, factory managers are able to employ predictive maintenance across heterogeneous devices on the factory floor. The data generated by sensors in pneumatic cylinders could be monitored in real time at the point of origin. Cumulocity IoT (installed on Dell’s Edge hardware devices) enables real-time reporting on machine latency times, alerts to prevent impending faulty productions, and reports about unplanned machine downtime
- New use cases deliver customer value with predictive maintenance, leakage detection and energy efficiency monitoring



Agriculture



The challenges

Agriculture is a mission-critical industry which has realised significant benefits from the usage of IoT solutions, and progress is set to accelerate via Edge computing. For example, Edge computing enables greenhouses to function as closed, intelligent Edge ecosystems — systems that do not need remote services and which can take care of themselves.

Edge AI can provide farmers with real-time insights, allowing them to identify areas that need irrigation, fertilisation or pesticide treatment. Precision agriculture uses AI technology to aid in detecting diseases in plants, pests, and poor plant nutrition. At the time of writing there is a shortage of agricultural workers, which makes AI and machine learning-based smart machines a viable option for many remote agricultural operations.

Applications

Vertical farming

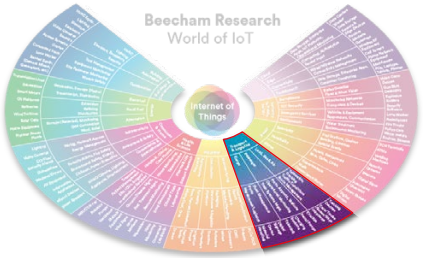
Predictive analytics

Crop & soil monitoring

Unmanned aerial vehicles (drones)

Crop planning.

Autonomous Vehicles



The challenges

Autonomous vehicles (AVs) take decisions in real-time and make extensive use of Edge AI systems, which are brought together in a central control unit. Autonomous vehicles are collections of dozens of 'things', cameras and sensors, as well as software systems, all working together to navigate and avoid pedestrians, cyclists, and other vehicles. AVs are de facto advanced, mobile IoT networks.

In addition to driving, AVs perform many more intelligent functions including recognising passenger identities, assisting passengers with limited mobility, and processing massive amounts of safety-critical data at the intelligent Edge. In addition deep learning is conducted in the cloud and 5G networks will facilitate the ability to make autonomous decisions in real time.

AVs have been deployed in controlled environments, e.g., mining and farming. The restricted nature of the operations there and the possibility to operate on private roads has facilitated adoption. Some benefits of autonomy in these sectors include savings in labour and reduction in carbon dioxide emissions. There are related deployments in the construction and warehousing sectors. Highway trucks are set to be the first vehicles to feature the full autonomous technology on public roads: prototypes already exist, and companies are currently developing the software algorithms needed to handle complex driving situations.

Applications

Vehicle-to-Vehicle (V2V) communications

Vehicle-to-Everything (V2X) communications.

In-vehicle safety, e.g., detect driver distraction and signs of drowsiness

Road safety: 90% reduction in traffic deaths

Environment: 60% drop in harmful emissions

Autonomous Vehicles

Case Study – LUCI Gives Wheelchairs Smart Driving Capabilities

Challenge

Approximately 1% of the world's population - over 75 million people - use a wheelchair on a daily basis. For those with mobility challenges, wheelchairs are considered a personal space, and represent freedom and independence in dayto- day life. But wheelchairs can be dangerous, with collisions, tip overs and falls commonplace, oftentimes resulting in serious injury. A case-control study found that in a three year period, 87% of wheelchair riders reported a tip or fall. Another study reported that in the last year that data was tracked, hospitals reported 175,000 emergency room visits from wheelchair accidents, 30,000 of which were serious enough to warrant admission.

Until now, there has been almost zero technology on power wheelchairs. Indeed most appliances, such as a toaster or coffee machine, contain more smart technology. LUCI uses similar technology found in autonomous vehicles, and while universities and research institutions are trying to build autonomous wheelchairs, LUCI's experience with many riders is that they are not interested in being 'driven' autonomously. Instead, wheelchair users want confidence, freedom and independence to safely operate their wheelchair on their own.

To help ensure the safety of the riders, LUCI wanted to create a connected solution that could send notifications to the wheelchair user or designated members of their support team for any potential hazardous threats or situations requiring assistance.

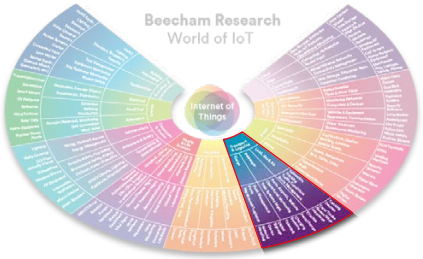
Solution

LUCI is a first-of-its-kind hardware and software platform, that attaches onto a power wheelchair. The device connects reliably to cellular networks using the Sierra Wireless HL7800 low-power wide-area (LPWA) module to help notify a wheelchair user of potential hazardous threats, while also sending programmed emergency contacts notifications about any falls and hazardous situations the wheelchair user is in. A low power solution was critical to minimize the impact on the wheelchair battery.

LUCI is installed between the power base and seat, and is compatible with two thirds of all wheelchairs on the market. It helps riders avoid collisions and dangerous drop-offs while maintaining personalized driving control. LUCI's cloud-based capabilities alert users and caregivers of low battery, possible tipping scenarios and other updates regarding the chair and rider. With LUCI, the wheelchair becomes aware of the user's reaction time, resulting in an improved user experience. The product is bundled with software including over-the-air updates, installation and data services.

LUCI is making wheelchairs smarter, safer and connected to real-world technology, such as Amazon Alexa or Hey Google devices.

Transport



The challenges

Safe, efficient, and reliable transportation of goods and people is essential for our global economy, whether it is by rail, road, water or air. To support economic growth and stability, transportation networks must be reliable and secure.

For the rail industry, IoT brings increased operational efficiency and an enhanced passenger experience. The benefits broadly divide into three key categories:

- Reliability and safety: breakdowns can introduce delays throughout the network. Deploying IoT sensors identifies problems with wagons and tracks proactively.
- Fewer Maintenance Delays: Predictive and preventive maintenance are more effective when smart sensors and data analytics are employed.
- Streamlined operations: Operators can control their trains more efficiently by tracking them across networks and processing the data using analytics.

We are seeing AI being used in rail applications to improve train scheduling, manage train speeds, avoid accidents, predict delays and enhance asset management. In addition AI can provide fast and convenient ticket-free check-in, accurate arrival-time predictions, personalised infotainment and onboard services, real-time track health diagnostics, and rapid response to an emergency.

Travellers are increasingly using combinations of different modes of public transportation and shared mobility. Railways are set to play a crucial role and pressure on the infrastructure is foreseen, especially in urban areas. Consequently, management and control of multimodal transportation pose serious challenges, to which AI technology can make a significant contribution.

Applications

Data driven applications enabled by AI's ability to process and interpret heterogeneous data from different sources

People-centric apps that understand and predict human choice behaviour and can persuade people to make better choices

Intelligent system simulation such as agent-based simulation to analyse the design and performance of mobility concepts.

Transport

SONY

Case Study – Ultra-Low Power Cellular IoT Chipset Opens New Opportunities in Vehicle Telematics

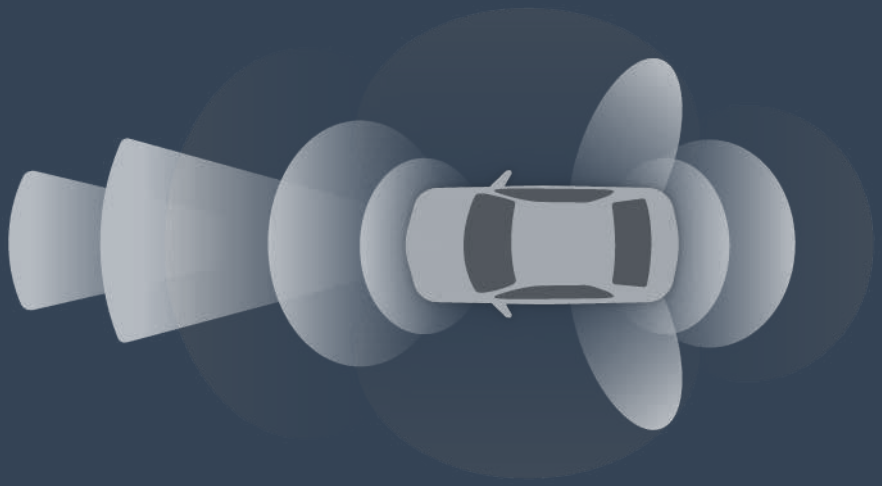
Situation - Vehicle telematics adoption is close to 50% today
Auto leasing companies and car dealerships need a reliable, long-lasting vehicle telematics solution to track, and potentially recover financed vehicles during the financing period. Legacy solutions that require wiring telematics devices to the car's power source make installation expensive and devices vulnerable to tampering.

Challenge - Assisting financing companies to track and recover vehicles
The challenge was to develop an install-and-forget vehicle telematics solution that would provide reliable, autonomous operation for the entire two-year leasing period – eliminating the need for device wiring to the car's battery and minimizing the risk of removal.

Solution – Sony's Altair cellular IoT chipset for the wire-free vehicle telematics device
Sony's Altair cellular IoT chipsets provide ultra-low power consumption, enabling vehicle telematics devices to operate autonomously on small batteries for over two years, cutting installation costs dramatically.

Results
By providing location pinpointing, speed notifications, pattern tracking, and much more, in a low-power, small, easy to install and conceal vehicle telematics device, financing companies now have a cost-effective & tamper-proof way to accurately track and recover vehicles when necessary.

Learn More
https://www.altair-semi.com/resources/vehicle-telematics-success-story/



Altair

Transport

WNDRVR

Use Case – Intelligent Systems in Automotive Industry

As we continue towards an even more connected and autonomous future, designing a vehicle is about creating quality experiences and customer desired outcomes, and software is at the epicenter of enabling this reality. Driven by intelligent connected systems, these experiences must make going from point A to point B safe, secure, efficient, entertaining, and convenient, and ultimately, autonomous. The current acceleration of new technologies is leading to unprecedented changes for the automotive industry.

With all this change, a new reality arises for OEMs. Being able to effectively manage software and ensure it lasts throughout the lifecycle of the vehicle is key. So the question becomes: How do you keep up with consumer expectations and extend the value and life of the vehicle without constantly adding cost, weight, power consumption, and complexity that eats away at your profits?

The answer involves taking ownership of software to deliver superior vehicle experiences both internal and external to the vehicle. OEMs are seeing the vehicle as a deployment platform for new software innovations. This translates to:

- Becoming faster and more innovative in creating software-driven services delivering great experiences
- Delivering more nimble and secure ways to update software, without inconvenience or disruption to consumers
- Breaking software to hardware dependencies, such that software and hardware can be introduced and updated independently
- Finding new ways to increase scalability, lower costs, and reduce timeframes between releases
- Facilitating communication connected cloud services, offering software-as-a-service, increasing automated operations, and using machine generated data to accelerate data driven actionable insights

Software has emerged as the common control point for the top trends impacting the auto industry—connectivity, electrification, shared mobility, and the rise of automated and autonomous vehicles. OEMs must prioritize owning their software strategy and the consumer experience, as well as be able to manage this process over the entire lifecycle of the vehicle, from ideation to end of life. This means thinking about the implementation of software in a way that lets the OEM fully control the inputs and the outputs.

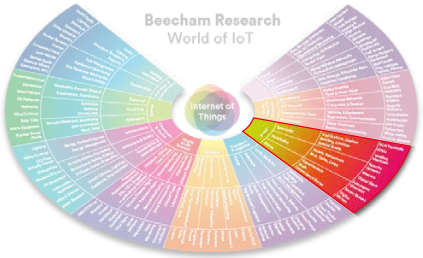
Enter Wind River Studio, our comprehensive edge-to-cloud offering for the development, deployment, operations, and servicing of safety-critical intelligent connected systems. Studio supports safety-critical applications that require real-time, deterministic performance and allows auto manufacturers to address a mixed-criticality environment.

For four decades, Wind River has provided software solutions across multiple markets where failure is not an option: automotive, aerospace and defence, medical, industrial, and telecommunications. In automotive, we bring software, technologies, tools, and services together with Studio to help the industry maintain the software systems of next generation connected vehicles across the lifecycle; our award-winning technology and expertise have played a significate role in the deployment of more than 100 million vehicles.

Wind River will play an important role in the transformation of the automotive industry by drawing from its heritage in mission-critical industries that demand the highest levels of safety, security, and reliability.

See also Wind River content in Section 4 – Using an Intelligent System for Autonomous Transport

Retail Automation



The challenges

Retailers are employing IoT technology to enhance customer experience, reduce costs, drive growth and improve overall performance. Sensors deployed in various Edge-based systems are used to monitor customer satisfaction, provide supply chain insights, monitor food safety, and monitor goods throughout the entire supply chain. In addition, tracking systems report related information such as location, temperature, humidity, and shock, thereby providing insights into quality control and traceability; these help to determine if materials are safe, delivered on time, and transported in optimum conditions. Perishable food spoilage and deterioration in the retail grocery industry results in a significant loss of profitability: the intelligent Edge permeates this sector.

The deployment of smartphone trackers on the retail's regular Wi-Fi network provides additional intelligence. They record the unique signal that each phone sends when it searches for a Wi-Fi network. This information is used to track customers and build a profile around their buying habits. For example: what time they came in and left; how long they waited in a checkout line; and how long they stayed in designated areas and what items were purchased.

Retailers are also using IoT technology to track lost shopping carts and baskets. In turn this app can help retailers improve customer experience by ensuring that they are always available. Relatively simple IoT solutions can help retailers ensure safety and compliance, for example, solutions that employ a people-counting sensor can be used to enforce physical distancing.

Applications

Personalised retail marketing and content delivery

Optimal staffing level indicators

Cashless and cashier-less payment systems

Movement tracking systems for optimal store setup

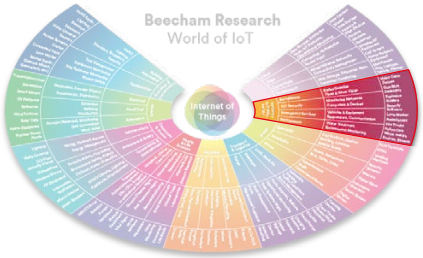
IoT-enabled warehouse robots

Wireless shipment tracking devices

Real-time condition monitoring of goods

Inventory management tools.

Public Safety, First Responders, Surveillance



The challenges

IoT applications bring greater situational awareness to first responders; they improve the speed and efficacy of emergency responses. As IoT systems are integrated into public safety systems, the technology's contribution to safety expands. For example, a traffic accident response team could use the data collected from a variety of Internet-connected devices such as those of the involved vehicles, the surrounding infrastructure, and the victims.

ETSI identified a number of use cases in which IoT devices could play a role in emergency situations. They included: Emergency Calling; Mission-critical Communications for situational awareness or to protect responder personnel; Mission-critical logistics support; and Public Warning Systems.

AI technologies can also be used to improve safety. Their potential to reduce, prevent and respond to crimes, for example, creates an opportunity to establish safer communities. As of the time of writing AI has been used for facial and image recognition, managing crime scenes and detecting criminal behaviour. AI and machine learning have also become critical technologies in information security because of their ability to quickly analyse millions of events and identify many different types of threats.

Applications

Preventative policing

Supporting criminal investigations

Number plate recognition

Running background checks

Real-time location sharing

Notifications of natural disasters and public emergencies.

Public Safety, First Responders, Surveillance

Case Study – High-Density Video Security

Challenge

The customer wanted to utilize technical innovations in machine learning, artificial intelligence, networking technology, and sensors to develop a surveillance system for all types of sites. The solution would include stationary components – such as surveillance towers – as well as back-end cloud infrastructure. The solution required secure and reliable high-speed connectivity.

Solution

The company designed a surveillance solution for perimeter and border security at various high-security sites. The solution has a minimal footprint and includes sensor and networking technology as well as solar power. Customers can deploy the solution quickly and it requires minimal support even in harsh conditions. The solution performs real-time analysis and filters data to optimize data transmission to the cloud. The company's cloud platform uses artificial intelligence, machine learning, and mesh networking to provide an accurate operating picture and integrates third-party data to provide complete situational awareness.

Hundreds of installations connect to the cloud platform using Sierra Wireless connectivity solutions. In North America, the Sierra towers are equipped with AirLink RV55 routers and Enhanced Carrier Connectivity. Enhanced Carrier Connectivity provides a competitive rate and cost-saving features from North American carriers. In Europe, connectivity is through Wireless Smart Connectivity. Smart Connectivity is a single, global, Smart SIM which accesses more than 600 partner LTE and LPWA networks in more than 190 countries. Each SIM currently uses 200GB to 500GB per month.

The company easily integrated the new SIMs into an existing fleet of SIMs, and all are managed on AirVantage, the Sierra Wireless connectivity management platform.

Benefits

By utilizing Sierra Wireless Enhanced Carrier Connectivity and Smart Connectivity, the company was able to quickly deploy a surveillance solution to provide perimeter and border security at multiple critical facilities and locations. Sierra Wireless services high-density, high-throughput video, which is then analyzed in the company's cloud platform to ensure safe and secure operations.

Public Safety, First Responders, Surveillance

SONY

Case Study – Ultra-Compact, Ultra-Low Power Cellular IoT Chipset Unlocks Pet Tracking Innovation Market

Developing the next generation pet tracker
A major challenge for the adoption of pet wearable devices is high power consumption and short battery life. Our customer, a top-rated GPS pet location and activity tracker device manufacturer, needed to develop a next generation pet tracker that could fit all pets and improve the current offering of one day battery life.

Overcoming limitations in terms of size, reliability and power efficiency
Our customer's previous tracker was bulky and less suitable for mounting on small pets. The device also needed to be recharged after one day. In minimum time, they had to develop a device that would be far smaller and last 10 times longer. As pets are considered part of the family, the pet tracker had to be 100% reliable.

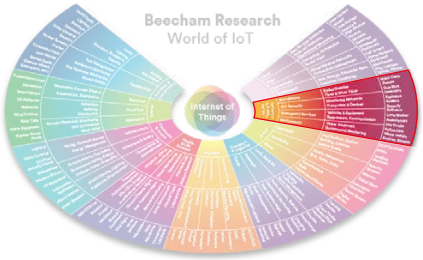
Sony's Altair ALT1250 ultra-low power, compact cellular IoT chipset
Our customer needed a mature core technology with a track record of stability and reliability. This is why they chose Sony's Altair ALT1250 cellular IoT chipset for their device. The ultra-low power consumption of our chipsets allows the device to last up to 20 days on a single charge, supporting continuous data analysis and communication to the cloud application. Its compact size allows it to fit easily and unobtrusively on a dog's collar. The cellular IoT connectivity in this cost-effective pet tracking solution helps pet owners quickly locate pets that have gone missing or gain insight into the pet's health and day-to-day activity.

Results
Our customer developed two products on time and met their KPI targets using eDRX operation and smart algorithms to track a lost pet while preserving the battery while at home. Sony's Altair dual mode LTE-M & NB-IoT cellular IoT chipsets were a key enabler of the customer's new products.

Many additional players are now developing a variety of animal trackers using our Cellular IoT technology. They believe that the simplified experience of developing their low power cellular IoT devices was thanks to Sony's Altair.

Altair

Water Utilities



The Challenges

IoT is being implemented in this sector to optimise water supply as well as distribution to help utility providers keep up with increasing demand. Smart meters provide near real-time information on consumption, which enables more efficient, demand-based supply and distribution.

Artificial Intelligence's ability to generate prediction information is enabling better demand forecasting; predictions can now go far beyond the weather, for example, how much additional water is used during a festive event.

AI can perform these complex tasks at speed and enable decisions to be automated and made in real time.

Applications

Improving distribution processes

Supporting demand management

Enhancing maintenance tasks

Transforming the customer experience

Case Study – Enabling Leak Detection with Cellular IoT, Helping Utilities Reduce Water Loss

SONY

Altair

Controlling water loss has become a priority for water utilities around the world. In order to improve their efficiencies, water utilities need to apply the right leak detection technologies.

Our customer is a pioneer in the development of advanced acoustic technologies, products and services that enable non-invasive diagnostics of the water utility pipeline infrastructure, including leak detection, pipe condition assessment and water loss management.

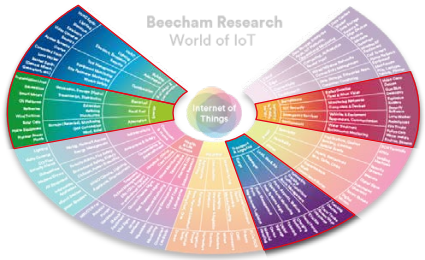
Our customer needed to develop a device which could be installed on a standard fire hydrant and could identify extremely faint acoustical noises emitted by leaks before they could be detected by conventional methods.

The device would need to be durable, secure, and self-contained - enabling easy installation in the water distribution network to monitor for leaks. It would leverage the existing fire hydrant infrastructure and would need to be compatible with multiple types and sizes of hydrants. The solution would include sensors, analysis software and power-efficient cellular IoT connectivity.

Sony's Altair cellular IoT chipsets provide ultra-low power consumption, extended battery life, reliability, and easy out-of-the-box experience, ideal for this acoustic leak detection device.

The company has completed hundreds of detection and monitoring projects globally for industrial and municipal clients, and with this new product, it can provide high quality and actionable information to water utilities, enabling them to optimize capital investments, repair and rehabilitation programs. This water metering solution also allows utilities to safely extend the operating life of critical water main assets.

Smart Cities



The challenges

Smart cities can resemble an enterprise operating in multiple sectors with government departments instead of divisions or groups, citizens as customers, and city employees and elected officials equivalent to corporate employees and managers.

Achieving cost savings and efficiencies is as important for cities as it is for enterprises and IoT edge applications can enable a city to do so. A city with efficient transportation, public safety, lighting, and other systems will also be desirable as a tourist or business destination, not just a place to live, with resulting tax revenue benefits.

A smart city is a responsive city, responsive to traffic conditions, emergencies of all kinds, and upkeep and maintenance. Real-time data sharing across city departments with overlapping responsibilities, possible in a city with a smart infrastructure, is one key to improved responsiveness.

IoT edge applications can also improve the ability of a city to comply with regional and national regulations. AI, Machine Learning, and data analytics have a place in smart cities as well, for example in traffic management and predictive maintenance.

Applications

Transportation

Traffic management

Coordination with bus, rail, and subway public transportation systems

Taxi regulation

Parking

Street and highway maintenance

Traffic lights, digital signage, street lighting

Public Safety

Fire, police, and first responder coordination

Environmental monitoring such as air quality

Water system monitoring and maintenance (drinking water, waste water, drainage systems)

Trash disposal

Notification of natural disasters and public emergencies

Video surveillance

Government Buildings

Heating, lighting, power management

Occupancy, social distancing

Municipal energy plants and power distribution

Maintenance and monitoring

Smart Cities

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.'

Smart Cities

Kigen

Case Study – Smart Tracking for Micro-Mobility in Smart Cities

Urban mobility is re-mapping the way we experience our cities
E-bike and e-scooter fleets have stormed from city to city in just two years, re-defining urban mobility and addressing some of the most vexing transportation challenges in cities congestion, emissions, air quality, and inconsistent access to transit. Research shows the sustainability benefits clearly: if the share for e-bike riding rises to 11 percent, we could see a 7 percent decrease in CO_2 emissions from the urban transport sector by 2030 – potentially accounting for over 50 percent of urban trips in the US and 70 percent in cities like London.

Behind the scenes, micro-mobility solutions are complex. They connect a diversity of stakeholders – government and city councils, product manufacturers, and platform operators – interoperability is important. Vehicle operators need a reliable, long-lasting solution to locate and retrieve lost devices or to re-distribute them to places of greater usage. Their success lies in the simplicity they present to the users, who will only change their behaviors if the services offered are significantly more convenient, trustworthy, and reliable. Those who sign up to use e-scooters also offer up a great deal of personal and sensitive data, including billing information and other involuntary analytics, such as location and individual vehicle information.

Challenge: Our customer is pioneer in the development of tracking and analytic solutions for managing and servicing large fleets of micro-mobility urban transportation. Our customer needs to support a unified experience for customers whilst meeting the regulatory, security and safeguarding requirements of multiple cities, across many regions. This required simplified manufacture of a low-power and compact cellular IoT enabled device that can be personalized to meet local needs and associated carrier profiles, which would allow to offer locate and retrieve functionality, reporting of lost asset, and collect utilization statistics to drive adoption.

Solution: Kigen's integrated SIM (iSIM) OS combined with our strong partnerships within the module and chipset ecosystem provided a route to simplifying secure manufacture and late-stage personalization eliminating the need for multiple product development routes and inventory management. To meet the needs of citizen data security, it was essential that these edge devices are treated with the most robust security protocols - implementing chip to cloud security with GSMA's IoT SAFE security scheme. This approach offers further assurances on ease of data cloud integration and interoperability.

Result: By simplifying the manufacture of cellular connected micro-mobility vehicles to offer location tracking, pattern tracking and further usability features in a compact, low power and ready to connect out of the box solution, vehicle companies now have a solution that can scale seamlessly. To ensure that the early benefits of greening our cities are realized, operators of fleets and city councils can take advantage of well-established security frameworks ensuring data of the city, it's consumers and all IoT that serves them is cost effective, secure, and tamper-proof.

Wider applicability: Kigen's iSIM OS and solutions are built with high-growth markets of Massive IoT, such that enterprises can leverage strong security even at the most constrained size, power, and cost envelopes. Through greater integration of components, longer battery life and tamper-proof protection can allow to safeguard IP and innovation for manufacturers. Much as large fleets of urban vehicles, Kigen's iSIM OS is enabling edge devices in consumer lifestyle products, in mobile medical healthcare devices as well as point of sale devices. This in combination with standards-based security scheme such as IoT SAFE is a perfect combination to support the market's growth and strengthen the social contract with users.

Smart Cities

SONY

Case Study – Solving Japanese Smart Gas Metering Challenges

Following the 2011 Great East Japan Earthquake, the Japanese government has mandated that 100 million buildings and households be fitted with smart meters by 2020. The government-initiated program, involving all Japanese telecoms operators, is for smart meter IoT, helping create an energy-efficient and low carbon society, by providing customers with information on their energy consumption and encouraging more efficient usage.

Our customer needed to develop a Cellular IoT solution that would enable continuous network availability and remote access, while allowing smart gas meters to maintain over 10 years of battery life in the field.

The meter should be accessible from the network – and be "on" to some degree, so that it could be remotely shut down in case of a tsunami or earthquake. Telemetering and robust communications were identified as key requirements for smart gas metering in Japan, due to a growing number of sites that were difficult for metering personnel to access. Other requirements included reverse-flow measurements, bi-directional information supply and enhanced security protocols.

Sony's Altair integrated LTE-M & NB-IoT chipset, ALT1250, was subsequently selected to provide LTE-M connectivity for LP gas meters in Japan.

Based on the Altair ALT1250 chipset, the company developed a cellular IoT solution capable of meeting the strict performance demands of network accessibility and battery life.

Sony's Altair chipsets now provide connectivity for all cellular-connected gas meters in Japan with continuous cellular connectivity.

Learn More
https://www.altair-semi.com/resources/smart-gas-meters-success-story/

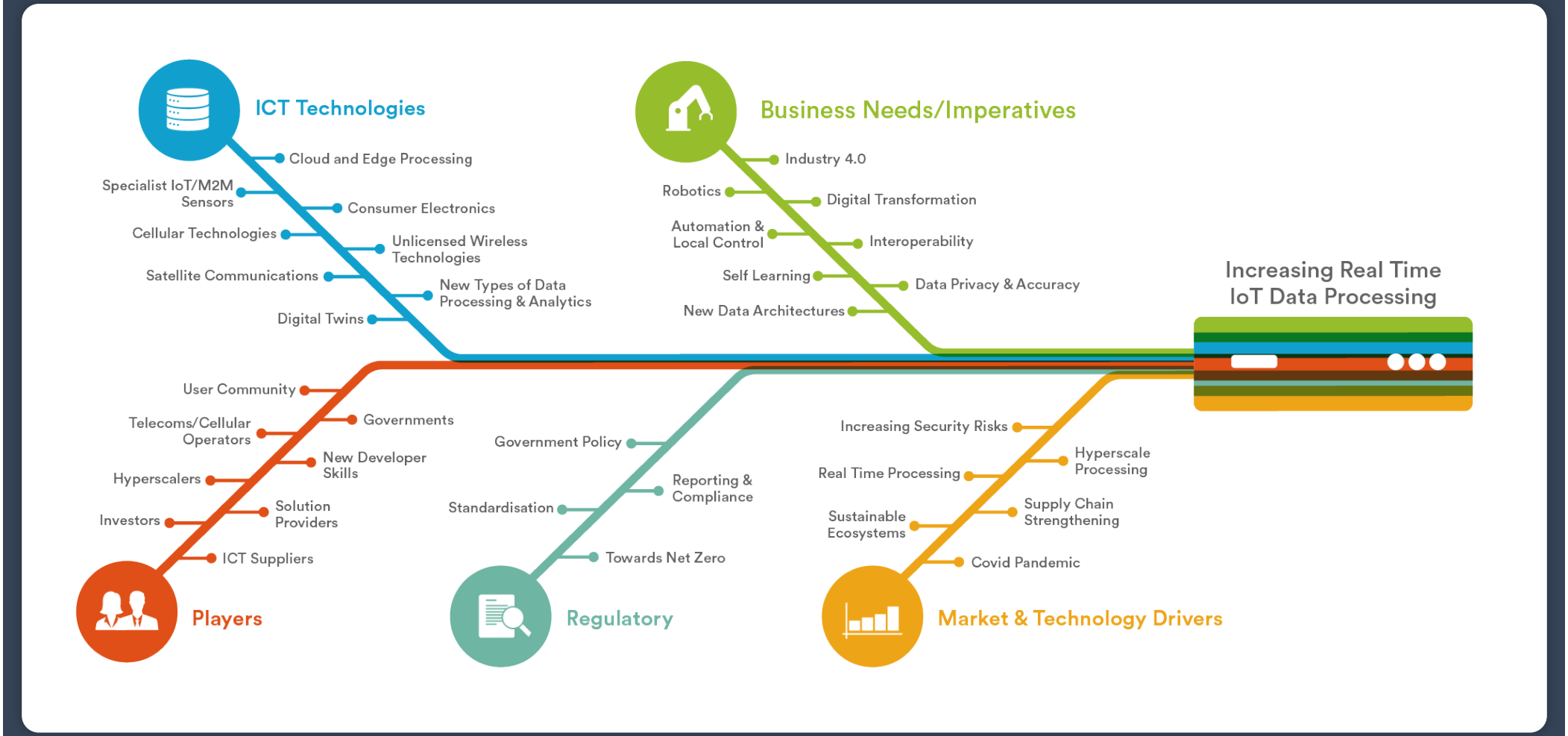
Altair

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, increasing real time IoT data processing.

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.

In this case we identify five main factors as follows:



Information and Communications Technologies (ICT)

Cloud and Edge Processing

Edge computing describes a distributed version of computation that brings data analysis closer to the data source. In a factory setting, this could see data processing take place at the machine level. 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.

Specialist IoT/M2M Sensors

Specialist IoT sensors are available in a wide range of capabilities, prices, sizes etc. to collect specialist data for applications in vertical markets as for example life signs (healthcare), dissolved electrolytes (water purity), particulates (air quality) and so on.

Consumer Electronics

The Consumer Electronics industry drives and keeps up with trends in smart phones, advances in miniaturisation, and the increasing use of wearables, as for healthcare remote monitoring and diagnostics.

Cellular Technologies

Cellular technologies are the primary wide area technology for collecting data from a wide range of devices across a range of industries; these have evolved over time and now cover 4G, 5G, private cellular networks, LPWA technologies, NB-IoT and Cat-M. These work over licensed spectrum and users pay a licensing fee, such that nothing will interfere with their transmission.

Unlicensed Wireless Technologies

With the exception of cellular devices (see above), many IoT devices operate in the unlicensed spectrum. Technologies in use for IoT include LoRa, WiFi, SigFox. In December 2021, the International Telecommunication Union (ITU) officially approved LoRaWAN as a standard. This move attests to its commitment to openness and standardisation, which are critical to achieving the interoperability needed for massive scaling.

Satellite Communications

The number of options for IoT using satellite connectivity has increased dramatically. Satellite imagery is increasingly used for applications relating to geolocation, environmental applications and examination of large areas including fields and woodlands.

New Types of Data Processing and Analytics

IoT systems are becoming more complex and the volumes of data are becoming almost unanalysable with conventional techniques. New tools like Artificial Intelligence (AI) and Machine Learning can help make sense of the data. There is however some debate as to whether new information generated from AI algorithms is as trustworthy as data collected at its source. To attest to this concern, the World Economic Forum has created the Global AI Action Alliance initiative to accelerate the adoption of 'inclusive, transparent and trusted' AI.

Digital Twins

Digital twins simulate the physical behaviour of an asset. They are used in the industrial design world as a way of optimally adjusting the qualities of a product before it is manufactured. A digital twin is not a simulation but a representation, and it uses real data from operating machinery and live processes to show what is happening.
Applications include Industrial Automation and Control, Retail Automation, self-fulfilment and warehousing and smart cities, and increasingly healthcare.

New Business Needs and Imperatives

Industry 4.0

Industry 4.0, or the fourth industrial revolution, focuses on how new and existing tools can be used in innovative ways. It is underpinned by a plethora of technologies including artificial intelligence, machine learning, IoT big data, robotics, augmented reality, 3D printing, drones, 5G wireless, and Edge and Cloud computing, all of which open up new possibilities and applications.

Robotics

Robotics are now established in every sector from manufacturing to healthcare and agriculture. The IoT and robotics communities are coming together to create 'The Internet of Robotic Things' where intelligent devices can monitor the events happening around them, fuse their sensor data, make use of local and distributed intelligence to decide on courses of action and then act to manipulate or control objects in the physical world.

Digital Transformation

The digitisation or digital conversion of business and industrial operations is ongoing. Several transformational digital technologies are contributing to opening up possibilities in industry, including the Internet and the Cloud, robotics and autonomy, blockchain, and additive manufacturing.

Automation and Local Control

Industrial Automation and Control goes hand in hand with real time operations and Edge computing. This broad-based sector is making smart machines smarter, factories more efficient, processes less wasteful, and production lines more flexible.

Interconnected Systems/Interoperability

Introducing greater connectivity in industrial systems has highlighted gaps in data exchange between the arrays of different systems that work across many operations. With data held in separate silos, the ability to exchange data and analyse a larger and fuller body of information is not possible. Interoperability for example assists in enabling different healthcare trusts to exchange key patient data.

Self-Learning/Self Adapting Systems

Self-learning systems enable data from across the connected environment to increase the accuracy and scope of predictions. Self-adapting systems react in real-time to changing conditions by making adjustments to meet goals.

New Data Architectures

The escalation of IoT data in terms of volumes and complexity has given rise to a plethora of new data management products such as data orchestration, data capture, data ingestion, data integration, data synchronisation. Data analytics techniques must make sense of IoT generated data , so that optimal decisions are made based on the results.

Data Privacy and Accuracy

Data privacy and accuracy is vital to maintaining the integrity of user information, protection from corruption, theft and so on. Data reliability plays a vital role in the increasing adoption of IoT devices; organisations can only make the right data-driven decisions if the data they use is correct and trustworthy. Conversely poor-quality data can lead to inaccurate decision-making.

Players

ICT Suppliers

ICT suppliers category includes suppliers of hardware, software, networking and communications equipment as well as systems integration and computing services.

Telecoms/Cellular Operators

Mobile Network Operators (MNOs) are essential for providing the connectivity service bundles and SIM cards central to M2M and IoT. They supply not only public cellular infrastructure and services to businesses and consumers, but also private cellular networks which can use licensed or unlicensed spectrum.

Solution Providers

We are listing solution providers under a separate heading as IoT solutions for the Cloud and Edge require highly specialised knowledge and multiple skills (see below under New developer skills) to develop IoT applications.

Hyperscalers

These provide very large-scale computing services and include international Cloud providers like AWS, Azure, Google, IBM.

New Developer Skills

Developers for new opportunities enabled by AI, 5G and the Edge must have the requisite skillsets for IoT application development including data science, hardware interfacing, IP networking and so on. These developers will shortly outnumber older programmers, and are said to prefer newer programming languages such as Python for Cloud and Edge architectures.

Investors

Investors including in the private sector provide funding for new R&D, applying data centric risk and opportunity assessment techniques to estimate the likely success of a capital venture. Good quality data is needed to better understand risks e.g. from climate change, fluctuating investment climate, financial factors, policy or technology changes or shocks in order to carry out impact assessment of risks. In 2021 14 percent of venture capital investment went into climate technologies.

Governments

Government agencies are stimulating adoption of new technologies through subsidies and projects. Government regulations change constantly as a result of new discoveries and policies.

User Community

The user community influences all industries that manufacture goods and provide services. It includes consumer pressure groups, which influence regulators, governments and producers. Consumer expectations change and in due course influence production, and loss of confidence in a particular product or service will have a huge impact on that industry. Good product designs will take into account the usability of that product by end users, such as wearables for healthcare.

Regulatory

Towards Net Zero Energy Reduction

The term Net Zero entails achieving a balance between the carbon emitted into the atmosphere, and the carbon removed from it. This will happen when the amount of carbon we add to the atmosphere is no more than the amount removed. To achieve this, emissions from industry will need to be cut, and this is now the focus of government regulation and industry concerns. The IoT can directly impact net zero targets through new insights in how energy is used to optimise savings.

Standardisation

The standardisation landscape changes continually for all industries and enterprises must keep ahead of the changes. With IoT systems becoming ever more complex, it is necessary for all parts to work together and interface effectively with each other. Interoperability is vital for all parts of a system which necessitates adherence to common standards.

Industry/Country Specific Reporting and Compliance

These requirements are specific to industries and to countries. Failure to comply will result in penalties. Data privacy and medical practices are examples.

Government Policy and Regulations

Government agencies are stimulating adoption of new technologies through subsidies and projects. Government regulations change constantly as a result of new discoveries, prompting changes in requirements and practices.

Changing Market and Technology Drivers

Covid Pandemic

In 2020, the world and industry were not prepared for the coronavirus pandemic. It has identified weaknesses in process supply chains and catalysed changes, and its effects are being assessed across several industrial sectors. For example, in the logistics industry even where goods are ready for delivery, there may not be the staff to handle them as they suffer from the disease themselves.

Future Sustainable Ecosystems

Long-term predictions indicate that the need to reduce resource use will accelerate. The pressures come from rising energy costs as well as from the cost and availability of materials and the security of their supply. Quite apart from the environmental pressures to be 'cleaner', manufacturers must reduce the consumption of materials and energy, and the subsequent generation of waste, in order to remain competitive and sustainable (Source: The IET).

Supply Chain Strengthening

With IoT-based manufacturing systems becoming more complex and requiring the timely input of components, it is important to strengthen supply chains nd make them responsive and resilient. Strong and sustainable supply chains help companies reduce costs, stock-outs and waste. By connecting goods, assets and people through monitoring, companies can improve supply-chain efficiency and unlock new revenue opportunities.

Real Time, Low Latency, Decentralised Processing

Companies that employ machine to machine communications to streamline manufacturing require real-time capabilities, where IT resources are deployed in close geographical proximity. This ensures that the data needed is readily available and there is low latency between production and the IT infrastructure.

Increasing Hyperscale

Hyperscale is about achieving massive scale in computing—as for big data or cloud computing. It allows an architecture to scale appropriately as increased demand is placed upon the system, by adding computing, memory, networking and storage resources to a set of nodes that make up a larger computing or distributed computing architecture.

Increasing Security Risks

Security is one of the major barriers to scaling IoT systems and all industries are at risk from cybercrime. The rapidly growing pool of IoT data is creating a huge and complex attack surface that makes enterprises and the wider economy more susceptible to threats. In depth cooperation and coordination between ecosystem members are needed to counter security risks.

Market Research and Analysis

What are the expected changes in the market from IoT at the Edge? This section examines this through exclusive interviews with senior industry management, survey results from several sources and analysis of key market trends.

Industry Expert Interviews

For this in-depth market survey we interviewed solution providers, familiar with all components of the solution, with customers spread widely accross industry sectors. Interviewees held a wide range of positions, from senior generalist (Chief Operating Officer, Chief Technology Officer, Chief Commercial Officer) to niche technical specialists (Director Experience Design, Verification and Computer Vision, DevOps engineer for Edge Computing).

Edge computing, Artificial Intelligence and Machine Learning solutions to enable customers to digitally transform by providing real time insights of business operations were examined. Comprising Edge intelligence devices including Distributed control systems, Control systems, Motion sensor kits, Robot arm controllers, IoT gateways and Industrial Personal Computers.

Some solutions provide Edge Storage as a service at global scale with methodologies for storing and retrieving data at the Edge; Edge Computing Virtualisation and Orchestration, Neutral Centric solution enabling flexibility and eliminating vendor lock-in; multi-Cloud and multi-Edge deployments etc. Some were very advanced, state of the art technologies allied to Edge computing, e.g. on device processing, security and device integrity for ML, AI and edge computing systems. Some claimed deep expertise in validation, advanced simulation and verification in the worlds of semiconductors for example. And some offered system on a chip units for the mobile computing and automotive market.

The following questions reveal all the insights we mined from this survey.

CLICK TO GO STRAIGHT TO THAT QUESTION

Question 1. IoT Edge drivers and trends

Participants in the survey are expecting a significant increase of applications at the Edge in the next 3 years. Digital transformation is the main driver.

Latency and Bandwidth are very important in real time applications and IoT Devices are growing very fast, generating large volumes of data. We are seeing a big demand in simplifying the deployment and delivery of low-latency applications and the ability to connect Edge networks between different regions and providers.

Another driver is GDPR, sometimes you need to have data processed and stored in a certain country or region and the Edge is great for that.

There is a strong technical case for embedded and edge abilities complementing connectivity, especially as networks become more complex and decentralised solutions are modernising infrastructure.

> ***Do you really want to stream that data to the Cloud, because there is cost, if you could process all that data locally and only stream the valuable data, that reduces costs. But I think the biggest driver that we are seeing is security.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration company

> ***The most prevalent trend is in reducing latencies. You reduce your latency just by having computing and data physically closer to users.***
>
> Computing Service Director of Developer Product and Relations
> Startup specializing in global Data Network and Edge

> ***We are seeing growth in these 3 areas: Industrial automation uses cases are growing fast – how to be more productive with less resources. Building automation, companies that manage buildings are trying to figure out ways to save energy. In the retail space, companies are looking at the point of sale and how to prevent thefts, bar codes visioning, to see if customers baskets match with receipts.***
>
> Chief Technology Officer
> Edge software solutions company

> ***The main drivers we see are advancing autonomous levels and acceptance of robotic solutions for personal transport such as scooter and bicycle rental without return to location and more home deliveries.***
>
> Verification and computer vision
> FIVE AI

> ***Driver; solutions need to be aware of environments and act to local changes quickly, clients asking for contained solutions, less data overheads.***
> ***Trends; rapid automation, co working robots, hourly changing batch production and warehouse use to facilitate on demand production and supply that has grown with the new widespread online cultures (business and private).***
>
> Development and Research Manager
> SMC

Question 2. Which use cases are developing fastest and why?

Edge has advantages in many verticals, industrial automation, building automation, retail automation. Asset health is a big area in manufacturing as well as predictive maintenance and planning maintenance actions on machines. Also industrial worker safety and preventive maintenance in oil and gas.

In retail, 2 major uses cases were highlighted, the logistics side and the retail outlet side. These uses cases are very interesting in terms are managing stores' fulfilments at the right pace. Intelligent cameras can detect low levels of stocks in real-time. Also surveillance for sales/demand forecasting, flow analysis, real-time advertising etc.
On the logistics side, real-time tracking of inventory. Monitoring temperature and freshness of products, predicting maintenance in large vehicles reducing downtime etc.

In E-Commerce and retail, if you manage inventories, you have to make quick decisions. If an item is not available it creates difficulties. Also, because of the pandemic, companies are investing in local fulfilment.

In healthcare, patient medical data and patient imaging is key. Bandwidth is one issue but it is mainly about privacy. Health data cannot leave the hospital, so must be stored locally.

Very many use cases include autonomous driving, information and transport network security, Public Safety and Security, Energy and Utilities, Rail and Transportation, Industrial Automation and Control.

> ***We see hospitals implementing our solutions that allow real-time image processing for disease detection.***
> ***Also Emergency medical use cases could leverage edge computing, data can be transmitted in 'near real-time' from ambulance to hospital.***
>
> Chief Commercial Officer
> Multi-access Edge Computing company

> ***In E-Commerce and retail, any lags on real-time distributed applications, your ability to load a shopping cart. A shopping cart is very interesting because it is very dynamic, you have no idea, what the person is putting in it.***
>
> Computing Service Director of Developer Product and Relations
> Startup specializing in global Data Network and Edge

> ***With retail analytics right now, we see a lot of cameras in stores, where the cameras are all across a store, trying to make heat maps of shopping patterns.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration

> ***Continued development of automation in dangerous and remote environments.***
>
> Development and Research Manager
> SMC

> ***Traditional use cases are isolated on site solutions but the arrays of distributed processing solutions are mushrooming.***
>
> System Validation Engineer
> ST microelectronics

Question 3. Key benefits Edge vs Cloud?

Participants believe that there is a space for Cloud and a space for Edge and those are going to co-exist in this hybrid Cloud/IoT environment.

Edge allows IT and OT communities to work together.

Edge offers several key benefits, where the data generated locally/on premises is happening in real time. The customer doesn't have to upload the data to the Cloud and then download insights later. You can reduce the load on your centralized system – improving cost, potentially. IoT devices create a huge amount of data and often you only use a small subset of data for long-term storage.

Regarding complexity, if you look at the Cloud, there are many options, most of which are geared towards IoT users. Business users, where the requirements are different, get less choice.

Functions such as AR and VR Training sessions can only be performed at the Edge, ensuring no lag.

Edge enables cleaning of data in real time, extracting valuable processed insights, shorter reaction times, adherence to local data stipulations and overall less energy and data costs.

> ***Moving large volumes of data to the cloud generates more cost than processing at the edge. Some medical images are between 2-8GB, you can't do it through cloud. It would be to slow and costly to use cloud.***
>
> Chief Commercial Officer
> Multi-access Edge Computing company

> ***Ease of deployment, in many cases the Cloud is very useful and very helpful because you can send anywhere in the world, but the Edge provides more flexibility/reactivity in your operations.***
> ***Edge is where the IT and OT are merging. For example in the network virtualisation, you still need IT and OT to come together so it can work.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration company

> ***Your taking load off your cloud and off your networks, because the data is being processed locally in an un-distributed fashion, so it is a cost benefit and a reduction of complexity benefit.***
>
> Computing Service Director of Developer Product and Relations
> Startup specializing in global Data Network and Edge

> ***We enable whole ecosystems with increasingly smarter chips. Integrating AI into products helps to make them smarter, reduce their energy consumption, but above all opens up new perspectives.***
>
> System Validation Engineer
> ST microelectronics

Question 4. How are AI and ML used at the Edge?

Automation stood out as the number one driver, at the moment, that is created or enabled by AI.

One example from the retail sector was using Machine Learning with labels or dimensions of packaging, that are scanned in real-time and quickly ingested into a database that compares them against how they should be, to make sure tolerances are aligned with quality standards.

Another example was detecting anomalies, data can be collected from machines that are on the shop floor, looking at patterns and training the machine learning model for patterns that would indicate that a machine is performing in an abnormal way.

Also video based analysis applications typically use AI and ML which can detect all sorts of hazards in industries where workers can be exposed to danger.

Both AI and ML are used increasingly as part of network automation as well as on devices or as part of IoT solutions. We see extensive use of ML and increasingly AI for computer vision, wayfinding, traffic pattern recognition, chat bots, manufacturing, warehousing, network security.

In the future we will see more bidirectional human to machine intelligence and a wider acceptance of shared services that require good experiences with often limited connectivity, distributed energy systems, a wide mix of solutions with fast response times and lots of data sources.

> ***We are seeing AI and ML taking a lot of data, in machinery with temperature sensors and vibration sensors. Running in an AI/ML system allows you to determine if the machine is more likely to breakdown. Also facial recognition at point of access in building. Vision inference can help with COVID regulations, the ability to know how many people are in a building in a square area.***
>
> Chief Technology Officer
> Edge software solutions company

> ***Pretty much every single use case receives a form of AI now. Its starts with a simple algorithm but they are becoming more sophisticated now over-time.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration company

> ***Real-time Machine Learning is all about optimising some sort of service in real time, and milliseconds matter.***
>
> Computing Service Director of Developer Product and Relations
> Startup specializing in global Data Network and Edge

> ***ML and AI can process x-rays and detect signs of chest diseases, such as COVID-19, tuberculosis etc.***
>
> Chief Commercial Officer
> Multi-access Edge Computing company

> ***In the future, expectations are that systems have intelligence, work together and can be operated by most people.***
>
> Software Development Manager
> NVIDA

Question 5. How do you see the use of digital twins developing?

Digital twins offer you the ability to digitally simulate an environment which is physically very hard to simulate. However it is felt that digital twins are still at an exploratory stage, a work-in-progress but less prevalent than other areas.

From the survey, healthcare and retail are currently the two strongest verticals for the use of digital twins but as data collection becomes more and more ubiquitous in the market there will be a lot of digital twins deployment in the next 3 years. Also, from a customer standpoint, it is easier to demonstrate the capability of a solution before deploying it. Digital twins can be used in addressing critical needs like the energy transition, with better data gathering and use.

> ***Digital twins will be an important element to deliver personalized medicine. Different health data sources can assist during a diagnostics. Laboratory results, imaging records, pharmacy data, medical records. Models can be created to detect symptoms before a patient is ill.***
>
> Chief Commercial Officer
> Multi-access Edge Computing company

> ***I see it as a key pattern on how we design solutions. It can be across all kind of industry verticals, they are relevant in Industrial and smart city context but also in entertainment, gaming.***
>
> Principal Technologist
> Startup specializing in global Data Network and Edge Computing Service

> ***What we find right now, each of the cloud providers offers digital twins. Digital twins require more interoperability and that the moment it is not quite there. We need cloud providers to recognize that.***
>
> Chief Technology Officer
> Edge Software Solutions company

> ***Digital twins have been around for a long time for defined processes and high end products such as chemical plants, planes and energy systems. They are increasingly used for harder to define fluid networks such as weather and behaviour patterns.***
>
> DevOps Engineer for Edge Computing
> DT infrastructure and servers

> ***The use of digital twins is widespread in global manufacturing with development and production often in different regions. The tactile internet is becoming a reality.***
>
> Development and Research Manager
> SMC

Question 6. Connectivity types and 5G

Companies looking at IoT at the Edge are mostly working on Private Networks, but 5G will have a big impact in terms of bandwidth to improve the spectrum and bandwidth that is available to enterprises. In this respect, 5G is going to be more like broadband.

The capabilities at the Edge that 5G operators will be able to provide to customers will also drive the adoption of IoT. 5G operators will be able to provide added services to end-customers, with better ease of use and fewer complexities.

From a manufacturing and industrial IoT perspective, 5G and Edge computing are probably going to be the most used/popular.

> ***5G will complement fixed lines, and this means better communication channels for the future.***
>
> Chief Technology Officer
> Edge software solutions company

> ***In the oil and gas industry, remote drilling areas that are far away from cables, 5G is very relevant there.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration company

> ***Private Networks provide more security, Oil and Gas industries in the US are using these networks to avoid hacking. Edge IoT devices when hacked can have devasting effects.***
>
> Director Experience Design
> Edge infrastructure

> ***4G LTE are often utilized in fleet management use cases. 5G would be particularly suited in more high density environments where you have hundreds of robots working together in factories.***
>
> Director Experience Design
> Edge infrastructure

> ***The scale out of connectivity and the ever faster changes in energy and transport are probably the most significant drivers for private networking and edge solutions.***
>
> DevOps Engineer for Edge Computing
> DT infrastructure and servers

> ***Unlicensed spectrum uptake has increased dramatically, it is a fast track for deployments where infrastructure does not reach. Wideband industrial spectrum is a real enabler for future proof edge solutions.***
>
> System Validation Engineer
> ST microelectronics

Question 7. Challenges in implementing IoT Edge solutions

Respondees cited physical security of devices as the highest priority when implementing IoT at the Edge. The devices are mostly remote, so companies need to take security into account to avoid hacking and malwares.

The second aspect was the readiness of companies to adopt Edge devices. When companies have grown their IoT and initiated trials, sometimes they have difficulties: will devices work together with their numerous compatibility issues? Can operating systems support IoT Edge applications?

From a technology standpoint, there are multiple choices when implementing Edge solutions. Narrowing down those choices can be a challenge. Also complexity in the Cloud creates challenges.

> ***Edge is where the IT and OT are merging. For example in the network virtualisation, you still need IT and OT to come together so it can work. We see ourselves having to work with the stakeholders in organizations' IT and OT and making sure there are aligned and they agree before we deploy projects.***
>
> Chief Operating Officer
> Edge Computing Virtualization and Orchestration company

> ***The focus is going to be on data orchestration rather than specific workload orchestration.***
>
> Principal Technologist
> Startup specializing in global Data Network and Edge Computing Service

> ***If you want to deploy an Edge platform you need to think about data security and connectivity that goes with it.***
>
> Chief Commercial Officer
> Multi-access Edge Computing company

> ***Maintaining own IoT networks can be a challenge. Edge solutions will improve deployment times and allow lighter devices. Main differences will come from on device embedded abilities to smooth out global differences in connecting to the edge or reduce the power consumption by reducing raw data transmissions.***
>
> DevOps Engineer for Edge Computing
> DT infrastructure and servers

> ***IoT edge solutions help to overcome challenges. The big challenge is to build ecosystems for the future. There are plenty restraints today and we should not leave more problems for tomorrow.***
>
> System Validation Engineer
> ST microelectronics

IoT M2M COUNCIL

The IoT M2M Council (IMC)

25,000 enterprise users and product makers that deploy IoT technology –
a platform for thought leadership, lead-generation, promotion, and research.

IMC EVENTS COVER...

- Edge Compute
- Private Networks
- IoT Security
- Low-Power Connectivity
- AI/Machine Learning
- New Business Models
- Consumer Markets
- CapEx vs. OpEx
- Industrial IoT

https://www.iotm2mcouncil.org/iot-library/event/imc-events/

User Surveys of the Market

There have been several user surveys published recently on the use of edge computing. In this section, we review findings from four of these relevant for this report as indicative of current thinking in this part of the market. These were from the following sources:

Eclipse Foundation
IoT Edge Commercial Adoption Survey 2021

Forrester
How 5G and Edge Computing advance IoT Value 2020

IBM
The Edge Computing Advantage www.ibm.com

IDC (focus on healthcare)
Edge Computing – Transforming healthcare by increasing resilience

CLICK TO GO STRAIGHT TO THAT PAGE

They contain user surveys that focus on:

- The future of adoption of Edge computing (including in conjunction with 5G)
- Perceived benefits of the technology and view of strategic importance
- Solution design issues
- User challenges and recommendations

Eclipse Foundation

The Eclipse Foundation's IoT and Edge Commercial Adoption survey published in 2021 aims to gain a better understanding of the IoT & Edge industry landscapes; it identifies the requirements, priorities, and challenges faced by organisations that are deploying and using commercial IoT & Edge solutions.

Some 300 business respondents were surveyed between January and March 2021 (base year 2020). These comprised organisations worldwide, including one third in the Americas, one third in Europe, Middle East and Africa, and one third in the Asia Pacific. Participants' roles were across the board, with the majority at executive level.

There was a wide spread of company sizes, 52 percent of responses came from individuals working in start-ups or small enterprises with fewer than 100 employees; 17 percent had 100-500 employees while 9 percent had more than 10,000 employees.

The industry sectors were across the board, but the Information Technology and Comms sectors comprised 41 percent of respondent pool.

Summary of the Findings

Adoption, growth, investments – deploying today (2020) or in the future

IoT and Edge are both growing in adoption by organisations. 47% of organisations are utilising Edge computing technologies today, and another 39% have plans to deploy Edge in the next 24 months.

Investment in IoT and Edge likewise shows an upwards trend in terms of amounts invested. While 54 percent of interviewed companies had made moderate investments up to USD100k, 30 percent indicated project spending between USD100k and USD1 million in 2020 (a twofold increase over 2019) and 16 percent anticipated spending of over USD1 million (a 25 percent increase over 2019).

Perceived benefits and strategic importance

35% percent of organizations indicated that decisions were being driven by staff at Senior Executive level, a significant increase from 18% in 2019; together with the fact that major decisions taken by IT personnel were reduced from 26% in 2019 to 21% in 2021,

Figure 3.1 *Organisation Size by Number of Employees*

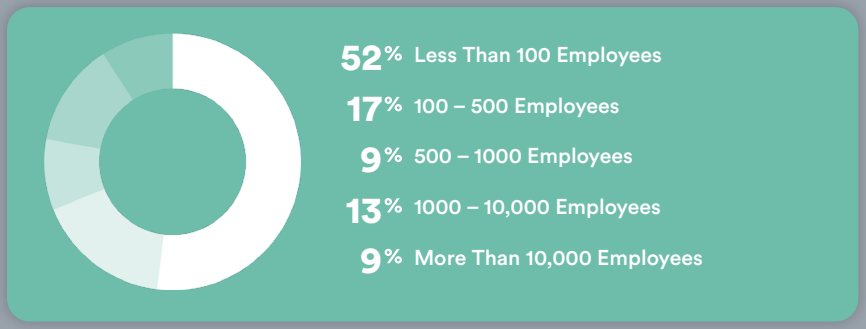


Figure 3.2 *IoT Technology Adoption*

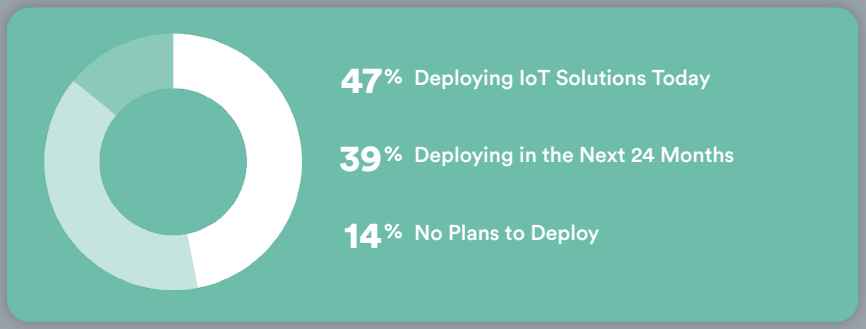
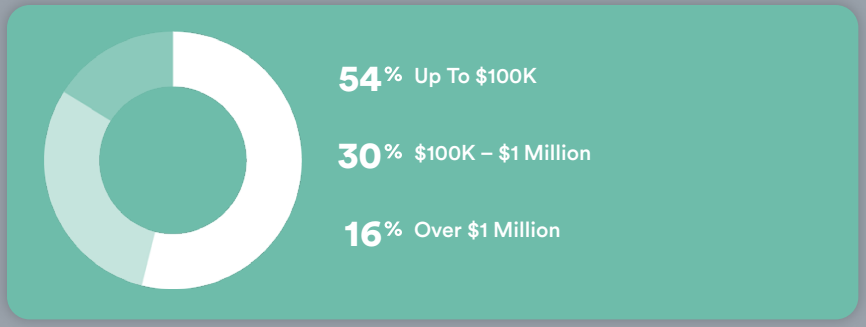


Figure 3.3 *IoT/Edge Investments 2020*



this suggests that Edge computing is now viewed as of strategic importance with more decisions made at executive level.

Solution design: – components of the solution
Cloud strategies: Hybrid IoT cloud strategies led the way at 44%, with Multi-Cloud following at 35%; Private/on-premises cloud infrastructure came a close third at 32%, with public cloud at 19%.

Components: Sensors, User Interface, Data processing and basic analytics were the most important technology components in the current IoT & Edge solutions.

Security: 36% of respondents saw Data Security as a primary design consideration when deploying IoT & Edge solutions, followed by Data Collection & Analytics 26%, and Connectivity 24%.

Open Source: 74% of organisations factored open source into their deployment plans. The decision was driven by the ability to influence or customise code in projects, cost advantages, and flexibility; specifically, the ability to customise or influence code in projects (29 percent); cost advantages (18 percent); as well as flexibility and agility (14%).

Adjunct Software utilised for the solution were Artificial Intelligence at 40 percent, followed by Control Logic at 37 percent, and Data Analytics at 30 percent; these made up the top Edge computing workloads organisations were currently running.

Challenges and recommendations
The top three IoT and Edge operational challenges were seen as

1. End-to-end IoT solution monitoring and management

2. Device management

3. Security (network/devices/data).

The survey concluded that data security and sovereignty should be implemented across devices and applications. Organisations must pay particular attention to their ability to retain control over data flow and storage, such as for data gathered from IoT sensors and devices.

Figure 3.4 *Cloud Strategies*

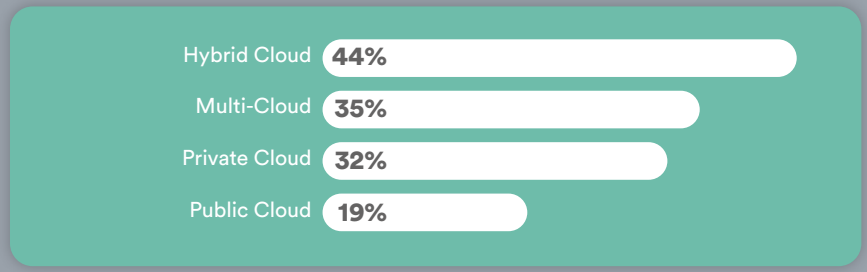


Figure 3.5 *Top Concerns for IoT Edge Deployments*

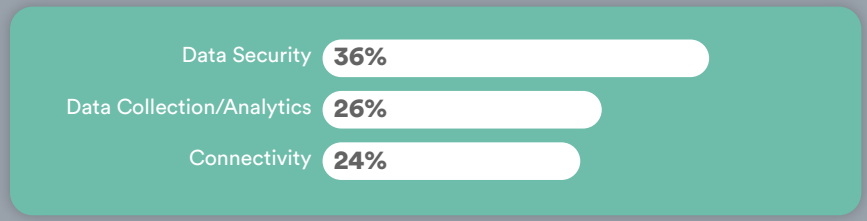
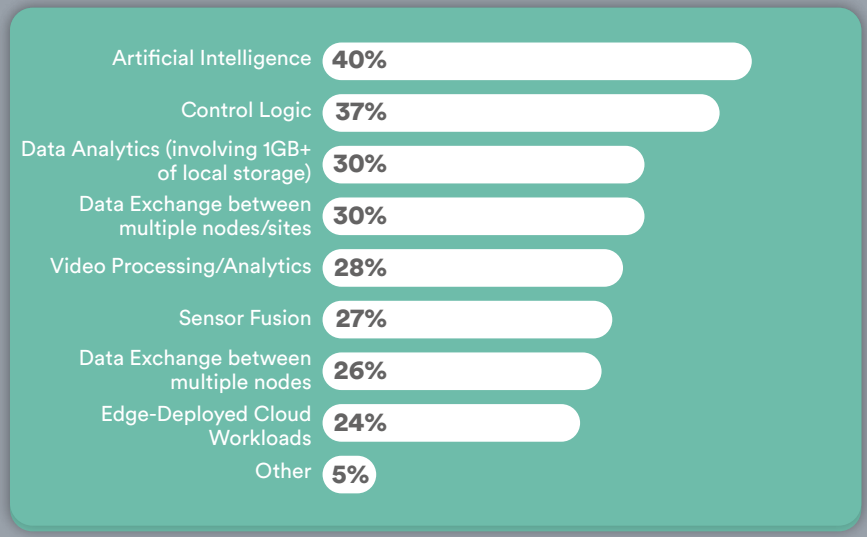


Figure 3.6 *Adjunct Software Utilised in the Solution*



Forrester

Edge computing definition: Endpoint and endpoint-enablement resources that manage and analyse localised data and empower near-real-time insights, engagement, and automation within physical proximity to endpoint devices and customers.

Summary of the Findings

Perceived benefits and strategic importance

- 5G powers IoT, automation, and Edge computing use cases
- 5G enables processing next to the connected device, using ultra low latency and ultra high bandwidth, and extends the breadth and variety of supported Edge computing use cases.
- Edge computing is helping solve previously intractable problems. It employs real-time AI across the physical/digital divide to solve previously unresolved business problems.

Overall Edge computing benefits include AI, processing power, low latency, and reduced costs.

Survey results

Base: 207 global mobility decision makers whose firm is implementing Edge computing (1,000+ employees); Source: Forrester Analytics Global Business Technographics Mobility Survey, 2019

Application areas examples:

Edge computing is helping solve previously intractable problems. Employ real-time AI across the physical/digital divide to solve previously unresolved business problems.

Retail: Drive better customer experiences and higher profits.

Healthcare: Diagnose and treat diseases with precision. Healthcare firms use private 5G and Edge to capture insight from connected facilities, equipment, and patient wearables.

Manufacturing: Drives increased production and revenue. 5G and Edge enable smart factory applications, value delivery.

Financial Services: 5G and Edge enable trust in financial services.

Figure 3.7 *Edge compute adoption in the year: 2020*

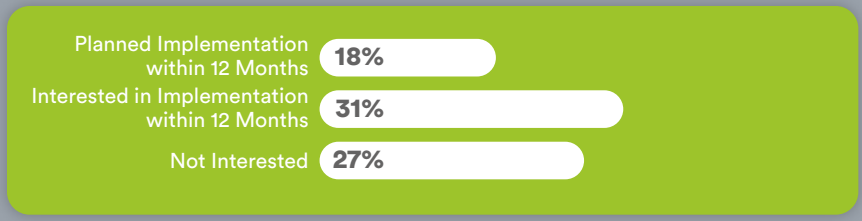
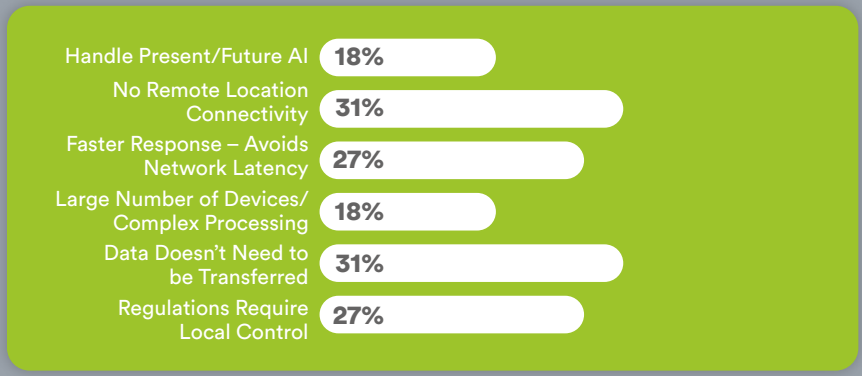


Figure 3.8 *Biggest Benefits of Edge Computing*



Transportation in route empowerment: 5G and Edge solutions enable multivehicle near-real-time aggregation and action enablement for safety and experience optimization.
Experience spaces – stadiums: 5G and Edge solutions empower spectators, athletes, and fans watching from home.
Public infrastructure: non-residential, remote business and government run locations involve land, water features, and permanent infrastructure.
Smart home: 5G and Edge use cases address entertainment, security, and home office environments.
Smart cities: 5G and Edge value delivery in cities: crime prevention
Edge compute: Equipment specifically designed and packaged for the purpose of near-real-time multi endpoint device content aggregation, analysis, and action enablement. Deployed at the endpoint on Edge networks; deployed in Edge gateways nearby or in the cloud.
Edge compute infrastructure: Management software, storage, CPU, GPU and bidirectional networking (to end devices / to clouds/DCs).
Edge intelligence fabrics: business logic, analytics, data flow and security.
Edge networking - Mesh networks, local Wi-Fi, peer-to-peer networking (e.g., Bluetooth).

Challenges and recommendations for Edge deployments

- Study the distinctions between what type of insights you need in real time, near-real time, and acceptably longer. Based on this analysis, look to spread your compute analysis architectures between endpoints, Edge gateways, and traditional data centre or cloud capacity.
- Use Edge compute to assess which collected data sets need to be/should be moved out to Edge gateways or back to your corporate traditional infrastructure. While 5G provides greater capacity, you'll still likely run into capacity limits on high volumes of IoT and mobile data sets.
- Focus Edge deployments and solutions on expanding customer values, especially in proximity to your most valued and largest customers. Don't lose sight of the overarching drive to win, serve, and retain customers.
- Align your 5G-enabled Edge priorities with a 5G network, data analytics, and deployment strategy.

Figure 3.9 *Components of the solution*

IBM

The IBM Institute for Business Value, in conjunction with Oxford Economics, surveyed 1,500 executives across 22 industries and 21 countries. This report focuses on the 140 chemicals, petroleum, and industrial products respondents.

Respondent roles were across the board. The survey explored their organisations' planned investments, expected benefits and impacts, and applicability of Edge computing across their enterprise and ecosystem.

Summary of the Findings

Adoption, growth, investments deploying today or in the future

Leading companies are leveraging edge today. These Edge Disruptors are embracing complementary technologies and focusing on select applications for edge computing. As the technology matures, adoption is expected to broaden quickly.

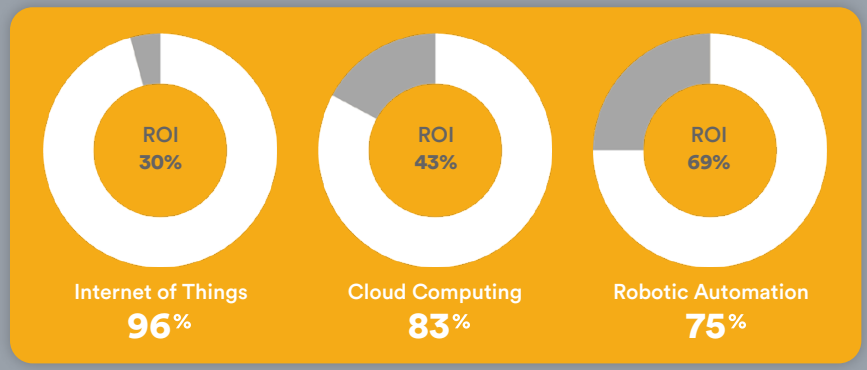
Almost two-thirds of organizations say they will invest in AI in the next 3 years to create new business models at the edge, combining intelligent workflows, automation, and edge device interconnectivity. They expect investments in edge computing to produce a positive ROI of 6.3% within 3 years.

The survey identified a subset of respondents we called Edge Disruptors. It selected them based on their expectations that;

1. Edge computing will have a positive impact on their organisational responsiveness
2. Their Edge investments would yield between 15% and 70% ROI in the next 3 years. Edge Disruptors today invest more than twice as much as their peers in Edge computing as a percentage of their technology budget (6.3% compared with 2.7%). As a result, they are further along on their Edge computing journey.

Edge Disruptors look to go beyond use cases and align with business objectives. Edge Disruptors expect to use intelligent machines to make harder decisions. More Edge Disruptors invest in technologies that complement Edge – and get more in return. Edge Disruptors plan to do even more with Edge computing applications.

Figure 3.10 *Edge Disruptors Embrace Complementary Technologies*



Perceived benefits and strategic importance

Edge computing can help energy, natural resources, and manufacturing companies take advantage of Industry 4.0 and drive productivity gains. By 2025, an estimated 38.6 billion connected IoT devices are expected to generate over 90 zettabytes – or 90 trillion gigabytes – of data. Sending this device-generated data to a centralised data centre or to the cloud can result in bandwidth, energy, and latency issues.

Edge computing is a more efficient alternative. With Edge, much of the data does not travel a network to the cloud or a data centre to be processed, significantly reducing latency – the delay in the transfer of data following a transfer instruction. Data can be analysed at its source, allowing organisations to make decisions and take actions based on the most current data at any point in time.

Recommendations summarised

1. Power and enhance data transfer – Explore and scale new technologies to power devices on the Edge.

2. Curate data to drive impact. Move from simply collecting data from every interaction (human, IoT, machine, and integrated) to using it to generate insights. Assess and prioritise the insights that deliver the most value.

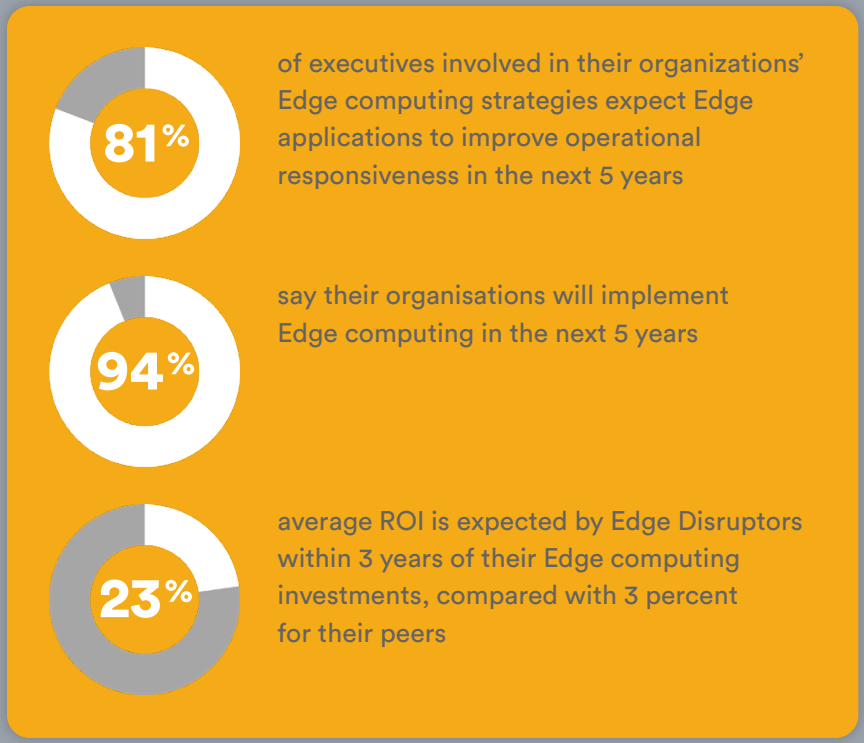
3. Bring the apps to the Edge. – Uncover ways to apply intelligence to operational functions and activities to power real-time insights that are decisive and actionable.

4. Act in real time. Use Edge capabilities for more immediate response and action.

5. Edge ahead of the competition. Achieve a competitive advantage with agile workflows and in-the-moment processing. Differentiate by providing customer, employee, and partner insights for responsive action.

6. Win big: Differentiate with speed. Investigate potential use cases where the combined power of 5G/private cellular and Edge computing can drive innovations, such as those requiring ultra-low latency and massive machine-to-machine data exchanges.

Figure 3.11 *Key Takeaways*



IDC

This survey was sponsored by Lumen Technologies and draws on IDC's Edge Services Thought Leadership Survey, September 2020

Summary of Findings

Adoption, growth, investments deploying today or in the future

Advantages of Edge computing include increased bandwidth, immediate access to data through latency improvements, reduced costs associated with transmission and storage infrastructure, and improved security.

Cloud computing and Edge computing are complementary architectures.

Edge computing architectures are highly dependent on business objectives. Telemedicine and virtual visits, clinical and business collaboration, the digital front door, real-time location services, emergency medical services, and smart medical campuses are enhanced with Edge computing.

Edge computing will play an increasingly important role in building operational resiliency to respond to the global pandemic and beyond in the 'next normal.'

Perceived benefits and strategic importance

Security and Data Protection Drive the Deployment of Edge Solutions.

Distributed Edge computing increases operational resiliency to cyberattacks because Edge computing presents a smaller attack surface than centralised cloud computing.

Protecting Sensitive Data Is a Key Priority for Healthcare Organisations.

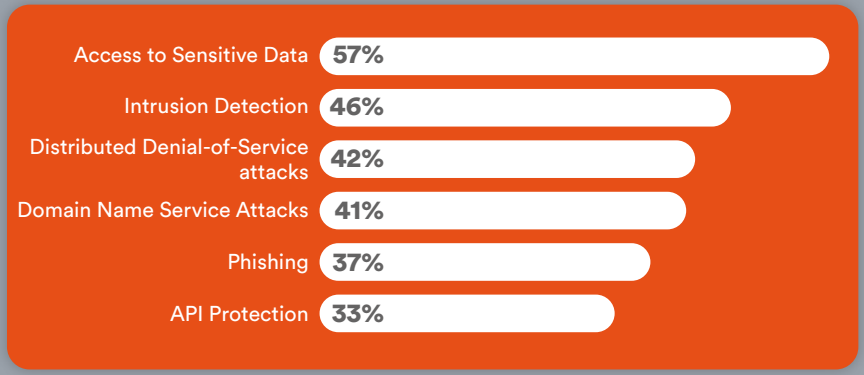
Privacy and security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) impose stringent controls over data access, use, and portability. Organisations that fail to protect personally identifiable information face steep penalties.

Managing Medical Devices at Scale Is Inherently Complex

The sheer variety of devices and the volume of data streaming from them creates challenges that can be addressed by Edge computing.

Figure 3.12 *Planned Investment in Edge Technologies*

Figure 3.13 *What types of security vulnerabilities are most important to mitigate*



Operational Resilience Is Essential for Mission-Critical Entities

Data is the lifeblood of healthcare organisations; downtime is not an option. As mission-critical entities, hospitals need to provide clinicians with secure, immediate, 24 × 7 access to electronic health information to enable expedient clinical decision-making.

Edge Computing Enables Superior Outcomes

Healthcare workloads involve large sets of structured and unstructured data that need to be accessed by care teams collaborating across the institution and, in the case of telemedicine, across the country. Downtime between systems or slow app performance is not an option.

Solution design

Healthcare organisations have made steady progress in embracing cloud technology. Because of security concerns, they tend to favour private over public clouds, especially for managing and storing sensitive data.

Moving workloads to the cloud and connecting to multiple cloud environments are major catalysts for deploying software-defined networks.

Challenges and recommendations

- Articulate a vision for using Edge computing
- Define key performance metrics for use cases
- Include stakeholders and domain experts
- Take inventory of devices already connected
- Embrace data governance, establish data definitions
- Take a holistic approach to security
- Seek a strategic relationship with suppliers

Figure 3.14 *What benefits do you expect Edge adds or will add to your organisation?*

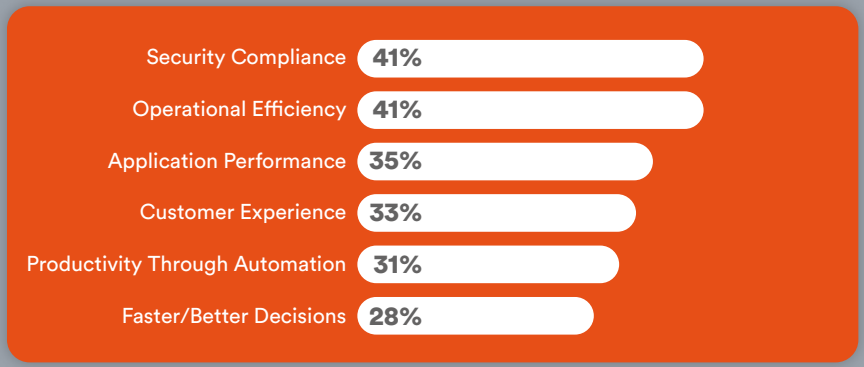
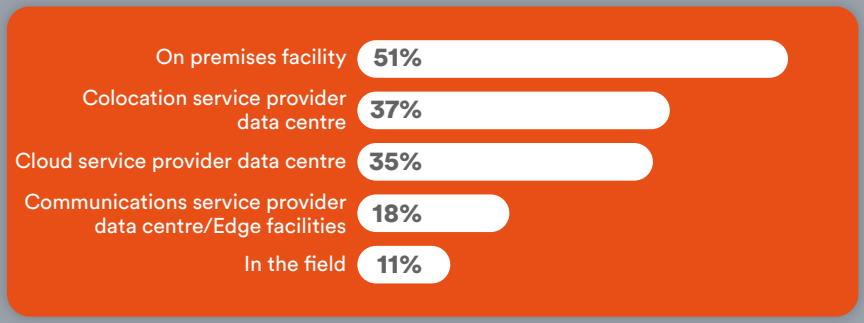


Figure 3.15 *Where does your organisation deploy Edge solutions?*



Conclusions

All four reviews are agreed that Edge computing is being adopted rapidly across all industry sectors, by companies of all sizes, and they cite a multiplicity of use cases.

Implementors see the technology of strategic importance to their companies. The benefits cited are commensurate with the properties of Edge computing, which include increased processing bandwidth, immediate access to data through latency improvements, reduced costs associated with connectivity and storage infrastructure,
and improved security.

Edge computing is viewed as complementary to Cloud computing, not as an alternative. Edge computing architectures are highly dependent on business objectives. The Edge computing facility is particularly important in cases where sensitive or commercially restricted data must be kept on site, for example in healthcare where protecting sensitive data is a key priority for healthcare organisations.

Edge computing solutions will increasingly include Artificial Intelligence components.

Market Overview

Significant Growth expected for IoT Edge

All parts of the edge market are growing. The pandemic has accelerated growth by heightening a need for remote capabilities even as a variety of technology developments have converged into a world in which distributed edge computing has become much more prominent. Market drivers include the need to process ever greater amounts of data and a need, in many use cases, for reduced latency – getting data to the cloud and back may take too long for a number of IoT applications.

The Linux Foundation (LI), in its State of the Edge 2021 report, forecasts edge market growth based on the power footprint (rated, not actual power consumed) of IT server equipment deployed at what it calls the Service Provider Edge, which includes the Access Edge (server-based compute at Telco network and edge exchange sites) and the Regional Edge (server-based compute at regional telco and direct peering sites):

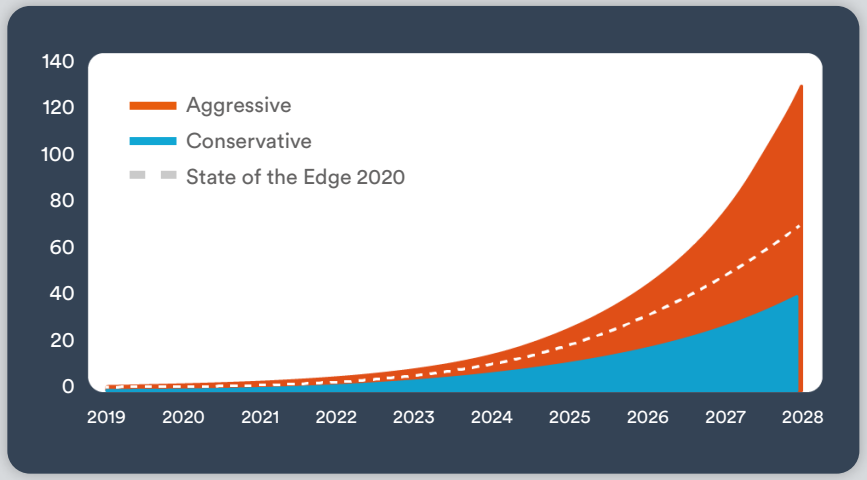
> **The global IT power footprint for infrastructure edge deployments is conservatively forecasted to increase from 1 GW in 2019 to over 40 GW by 2028, with a CAGR (Compound Annual Growth Rate) of 40%**

The optimistic/aggressive forecast option is for about 130GW by 2028. These forecast options are shown in Figure 3.16. Clearly, IoT at the edge is set to be a major factor in the market over the next few years.

Not included in this forecast is the other main edge tier the report focuses on – the User Edge, consisting of:

- Self-contained end-point devices, such as smart-phones, wearables and automobiles;
- Gateway devices such as IoT aggregators, switching and routing devices;
- On-premises server platforms.

Figure 3.16 *Total Global Infrastructure Edge IT Power Footprint from Linux Foundation's State of the Edge Report*



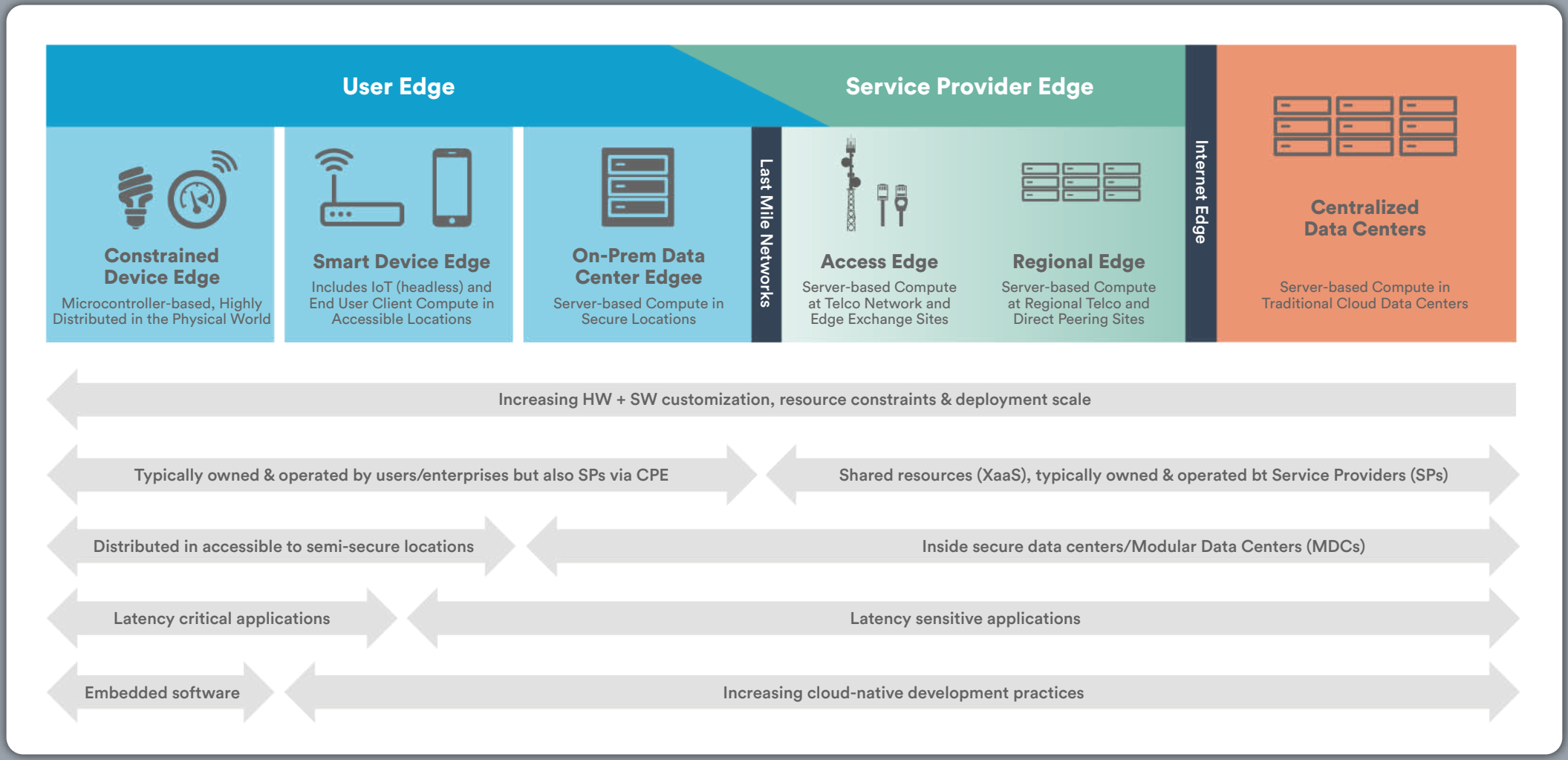


Figure Above shows LI's Edge definitions. Different sources segment the edge in different ways and may use different terms. Near Edge refers to near telcos' central offices; Far Edge to devices and sensors but also cell towers, part of the Access Edge as generally used. Constrained Edge is also referred to as Thin Edge and often involves battery powered sensor or devices used for applications producing limited quantities of data, such as tracking. Thick Edge refers to applications and devices using large quantities of data and/or requiring significant computing capabilities.

Figure 3.18 shows LI's forecast broken down by sector. It is important to note that these figures relate to all IT and IoT services, not just IoT. In particular, Mobile Consumer and Residential segments are in fact substantially not IoT related at this time.

IoT Edge also features in Boston Consulting Group (BCG)'s The Battle at Computing's Edge report. BCG segments the edge market into four categories:

- Device Edge: Onboard signal and data processing
- Premise Edge: On-premise infrastructure
- Access Edge: Network access points including cell sites and access points of presence
- Metro Edge: Major regional aggregation points

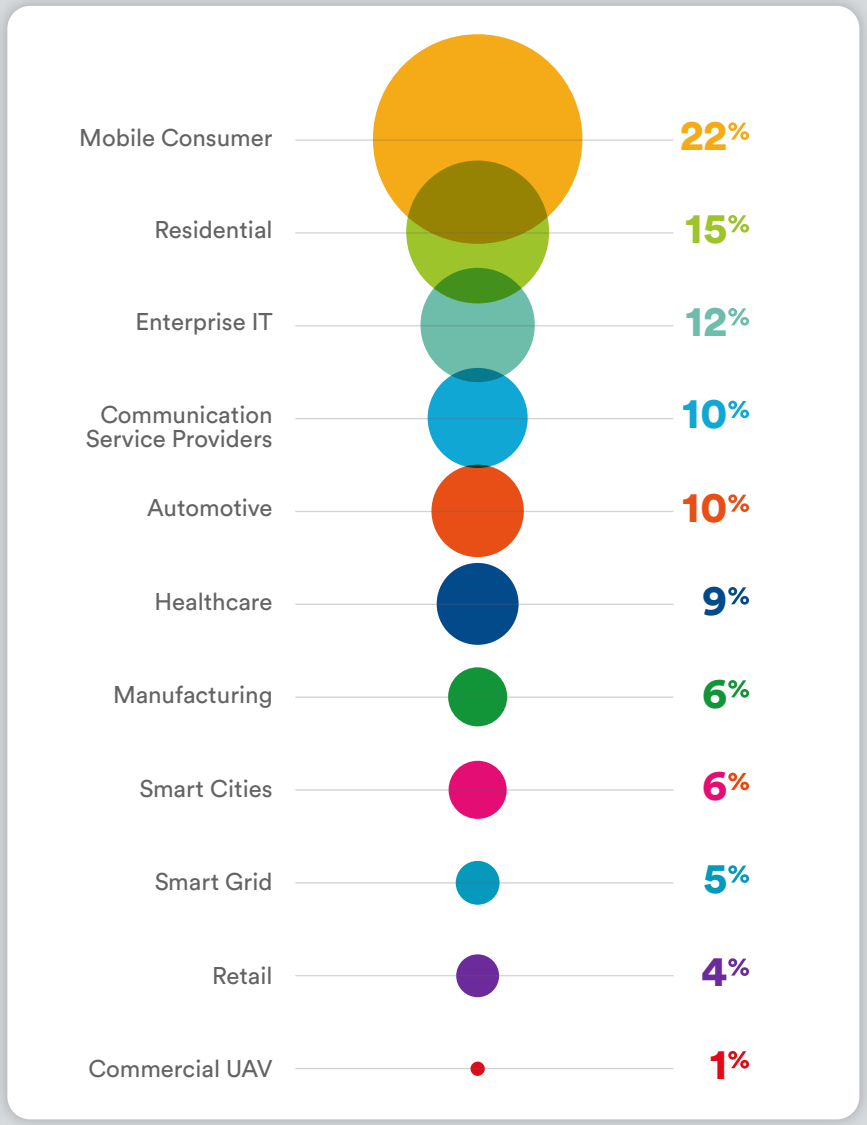
They also project strong growth in the overall IoT market – doubling from 2019 to 2024 'and driving significant growth in the edge IoT market' adding: '…we expect the edge to grow by 35% annually and the top edge use cases to represent over 20% of the IoT market in 2024, compared with less than 10% in 2019.'

BCG adds: '…the device edge and the premise edge currently make up about 75% of the market. Beyond 2024, as 5G and other advanced networks roll out, we expect growth in the access edge and the metro edge to accelerate.'

In addition: 'If the edge is viewed as a stack of services, software, and hardware, each of these layers is likely to grow by at least 30% a year. The applications and analytics sublayer will continue to be the largest slice of the market through 2024, while the hardware layer is likely to be the fastest growing.'

Other sources indicate similar levels of growth in IoT Edge over the next few years.

***Figure 3.18** Linux Foundation's Global Infrastructure Edge Power Breakdown*



Conclusion

A primary benefit of IoT edge computing is low latency. In addition to enabling new applications, this will increase the speed of existing applications and reduce costs in multiple ways such as reducing data transport costs and accelerating responsiveness. Edge also offers the possibility of improved reliability, security, and convenience.

Cost reduction, increased responsiveness, improved reliability, security, and convenience: These contribute to desired business outcomes.

'Whether it's an operator eeking every bit of efficiency out of its network while offering up new services or an enterprise turning data insight into cost-saving/revenue-generating action, time to action corresponds to time to value.' Sean Kinney, RCR Wireless.

These are major factors in the growth of the edge even as forecasted growth will likely lead to lower costs of edge infrastructure, which will also factor in that growth in a kind of feedback loop.

An awareness of growing edge markets is essential for charting the future, whether for enterprises or product manufacturers – which applications will it enable? How will it impact existing applications? Which capabilities will become more efficient? Which components will play important roles?

IoT Solutions and the Growing Edge Market

The overall IoT and Edge markets overlap in many ways, with developments in each market area impacting the other. Consider just one recent development in the Access Edge: The creation of small data centers at the bases of cell towers in the U.S. and Europe. These do not just benefit consumers watching streaming media on smart phones – along with the rollout of 5G, they will also play an important role in reducing latency for mobile cellular IoT solutions, including emerging applications such as AR, VR, UAVs, and semi-autonomous vehicles.

The expected high growth of IoT edge will be reflected in the elements that form parts of IoT edge solutions. These include:

- Edge to cloud connectivity
- As part of cellular connectivity, the use of eSIM/iSIM
- Connectivity hardware – intelligent routers and gateways
- IoT security

A related area is also Digital Twins. IoT edge solutions offering real time operations are also set to transform how many enterprises operate. Beecham Research refers to this as the Real-Time Enterprise. Others use different terms, notably **Wind River's use of Intelligent Systems** as outlined in this report.

Edge-to-cloud Connectivity

A decade ago 4G/LTE was a breakthrough development, much more than a step up from 3G. Now it has evolved into a comprehensive set of communications services offering Gbps data rates, low 50 ms latency and customised connectivity. 4G/LTE has become the networking technology that is delivering the demanding wide area connectivity requirements of IoT use in business. Those requirements include connecting staff, devices, vehicles and applications in all industrial verticals. IoT at the edge has a major part to play in this.

IoT in business operations has the proven ability to boost operational efficiency, improve product and service performance, and enhance operational agility particularly at the edge.
The overall result is a significant uplift to a company's competitive offer and its bottom line.
IoT has truly moved from 'nice-to-have' as a low cost remote monitoring activity to 'strategic necessity' in many business operations as the emphasis moves more towards control and automation. This trend is set to continue at a fast pace over the next decade. At the same time, the IoT market is moving to 5G, which offers yet more new opportunities for use of IoT in business.

In particular, IoT-specific 5G generic services will drive the use of edge IoT. These are:

- Massive Machine Type Communications (mMTC)
- Ultra-Reliable Low-Latency Communication (URLLC)
- Enhanced Mobile Broadband (eMBB)

mMTC will enhance low power wide area (LPWA) technologies and enable high volumes of IoT devices to be deployed in dense populations (upto 1 million devices per square kilometer). URLLC will be suitable for a number of mission-critical IoT applications with low latency requirements. eMBB addresses use cases requiring high data rates across a wide coverage area.

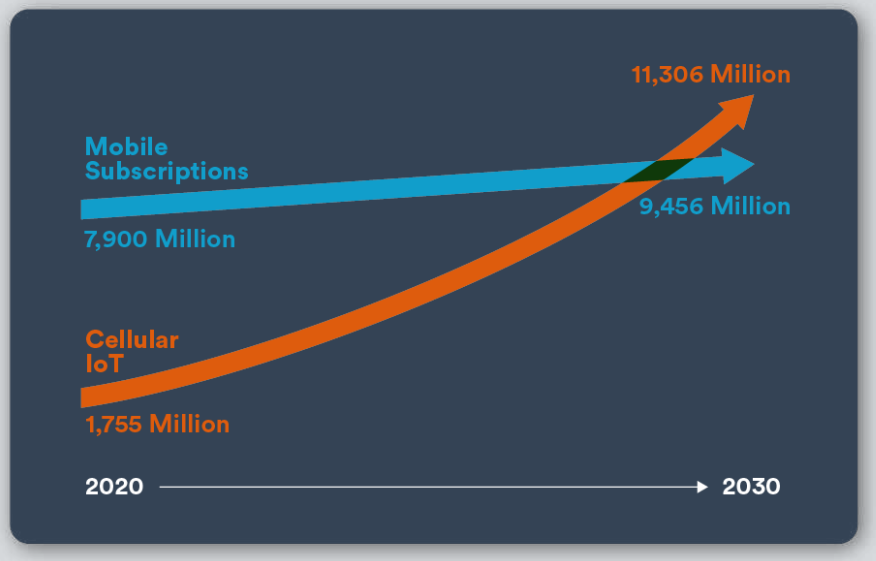
5G and edge computing are then inextricably linked. Low latency of the order envisaged with URLLC can only be provided with edge computing. So, the introduction of 5G will naturally accelerate the shift to edge computing. This also creates the need for standards at the edge to ensure open systems where different vendor solutions can interoperate at the edge. This has given rise to the Multi-Edge Computing standards work of ETSI (European Telecommunication Standards Institute).

So what does that mean in terms of numbers? Taking an overall view, for one thing while the projected growth of mobile handset subscriptions in the decade 2020-30 is expected to average 1.8% CAGR, the equivalent for cellular IoT connections is expected to average 20.5%. In other words, by the time we get to 2030, there are likely to be more cellular IoT devices connected to mobile networks than mobile handsets.

This is an indicator, but it is not the whole story for IoT . One thing is for sure – business operations are increasingly relying on IoT and cellular IoT in particular.

The increasing use of edge processing in IoT will reduce the growing need for high bandwidth connections to the cloud, while accelerating the need for lower bandwidth connections, all of which are provided by **Sierra Wireless as detailed in this report** For cellular, this includes NB-IoT and LTE-M/CatM1, the chipsets for which are provided by **Sony Semiconductor, as also detailed in this report**. In turn, this increases the need for more automated forms of connectivity provisioning and deployment – more automated and less manual intervention. This points to embedded SIM (eSIM) and integrated SIM (iSIM) as being of increasing importance for deployment of edge IoT cellular connections.

Figure 3.19 *Projected Mobile Subscriptions vs Cellular IoT Connections*



eSIM and iSIM

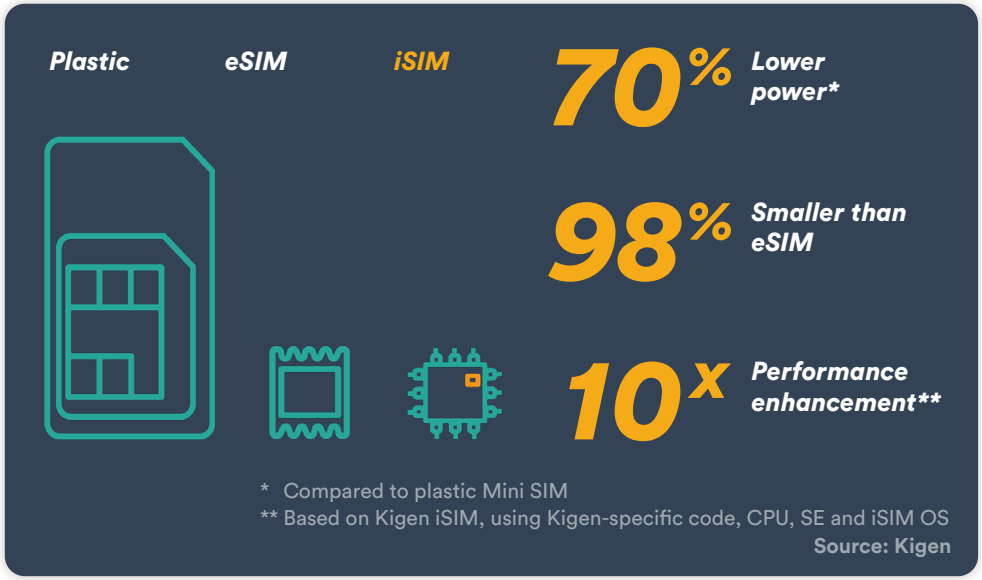
The tradition Subscriber Identity Module (SIM) card, used for cellular network authentication and initially developed for consumer mobile phones, has evolved over time, including smaller form factors. Unlike mobile phones, most IoT solutions are built on location and this creates significant logistical issues to ensure the right SIM card is matched with the right IoT device in the right place, particularly where international deployments are involved. SIM cards also present significant physical security risks and are not ideal for physically demanding environments.

The eSIM solution was developed in response to the limitations of traditional SIM cards for IoT. Initially deployed in the supply chain for connected cars, their use now extends to a majority of IoT applications. The eSIM solution specification enables remote provisioning of network profiles, a great improvement for managing the connectivity of large IoT deployments. As part of the solution, the Universal Integrated Circuit Card (eUICC) is typically soldered to a circuit board, is tamper-proof and better protected from extremes of vibration, temperature, dust, and other environmental challenges. This creates the opportunity for a smaller form factor for the connected device, with no need for a SIM card slot or tray which then also reduces the unit cost. All of this means that a device with eSIM solution can be manufactured as a single stock keeping unit (SKU) for use in multiple geographies with the correct network profile being downloaded at the point of use. Because of these benefits compared with traditional SIM cards, eSIM solutions that comprise eUICC chips and the Over-the-Air (OTA) provisioning system are expected to represent over 70% of installed cellular IoT connections by 2025.

Into this mix, the integrated SIM (iSIM) has been developed as an evolution of eSIM where the physical SIM sits inside a secure element within a System on Chip (SOC). This removes the physical component from the device circuit board, reduces power requirements significantly and also improves security compared with the eSIM solution.

Figure 3.20 shows a comparison of the traditional plastic card SIM, eSIM and iSIM. As is evident, the iSIM solution is particularly suited for resource constrained devices where there is limited power and where there is a need for a small overall device form factor. A wide range of solutions across many different sectors, including Buildings, Energy, Consumer/Home, Healthcare, Industrial, Transport, Retail and Public Safety are now envisaged. This includes fully functional AI and ML based edge devices as well as highly constrained form factors. **As covered in this report, Kigen** is working together with partners to offer secure IoT with a standards-based approach to Integrated SIM (iSIM) and eSIM technology.

Figure 3.20 *Comparison of Plastic SIM, eSIM with iSIM*



Kigen

IoT GLOBAL AWARDS '21 WINNERS

Kigen TELECOM INDUSTRY 2021

Future Digital Awards Gold Winner Technology & Innovation Awards 2020

The future belongs to those **re-thinking the possibilities**

Security is the foundation of trust in our digital society. At Kigen, we are making eSIM and integrated SIM (iSIM) the cornerstone of security.

Take advantage of future-proof, flexible, hassle free eSIM and iSIM technology.

- Compact and code-efficient OS across SIM, eSIM and iSIM
- GSMA accredited remote SIM provisioning server solutions
- Extensive ecosystem of innovation and full range of services to support your success
- Built for the secure and intelligent IoT edge of the future

For more information, visit kigen.com/solutions

Recognised as "Best IoT Security Innovation of the Year 2020" by FDA Awards.

Recognised by CIO Review as the Most Promising Technology Company for Telecoms in 2021.

Intelligent Routers and Gateways

Edge computing processes and analyses IoT data at or close to the source in near real time, thereby enabling more autonomy and the the creation of new services – for example predictive maintenance programs and allowing operational and management decisions to be made quickly at the local level.

Cloud computing processes and analyses IoT and related business data at a central facility. It is used for the analysis of “big data”, to find hidden patterns, correlations, market trends and customer preferences. Combinations of edge and cloud data analytics enable predictive analysis, which is used to determine patterns and predict future outcomes and trends.

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. In turn, this has enabled edge computing to perform low-latency data analysis tasks that were previously undertaken by the cloud or a private data facility. Computing resources that perform advanced data analytics tasks are embedded in both the IoT devices and the edge hardware such as intelligent routers and gateways. The edge hardware provides both connectivity and data processing capabilities at the speeds needed to identify and route critical data in mission critical applications. These devices are programmable, enabling developers to optimize their functionality to support near real-time applications.

The next step, empowering these edge products with Machine Learning (ML) and Artificial Intelligence (AI), boosts their ability to process and analyse data, a development that is enabling the creation of innovative applications such as machine vision and voice recognition. Until recently it would have been impossible to run AI locally as the hardware size and cost would have been prohibitive. This intelligence shift, towards the edge of the network, enables the centralised cloud to be used for computationally intensive tasks, for example to analyse bigger data sets and employ advanced analytics for tasks such as generating recommendations and discovering deep insights. In this way, edge and cloud computing still perform complementary, symbiotic roles, but now they are different. AI has reset the edge-to-cloud model.

IoT Security

A recent report by Economist Impact for NTT (dated December 2021) found that 69% of executives agree that the security of their current infrastructure is not strong enough. With ransomware on the rise, executives are looking for ways to improve defenses against increasingly sophisticated attacks.

The interviews conducted for this report and covered earlier in this Section also confirm the increasing concern for IoT Security. As IoT moves to the edge, with increasing relevance for local control and automation, it is becoming increasingly involved with business-critical operations. As a result, IoT security is becoming increasingly essential. It is also of fundamental importance that new security features do not lead to closed, proprietary solutions. Such a direction would inevitably work against efficient sharing of important operational data between different systems – a fundamental IoT principle.

It is therefore inevitable that security frameworks are required that provide for high levels of overall end-to-end security but with sufficient flexibility to ensure efficient and open interoperability between different supplier solutions. Such a framework is provided by **PSA-Certified, as covered in this report**.

Digital Twins

Digital Twins is a software application that can model and/or simulate a single device or large deployments of devices and entire processes and systems, by creating real-time digital counterparts. As such, it is closely related to edge IoT. The digital twin market is growing rapidly per forecasts -- Grand View Research for example predicts a growth rate of 42.7% CAGR between 2021 and 2028, after a pandemic-related slump when plants and facilities closed, growing from $5.04 billion in revenue in 2020.

There are many kinds of Digital Twins and all present versions are proprietary. One indication of the rapid growth of their market is the existence of at least eight organizations focused on standards and/or market development including the OMG's Digital Twin Consortium, which has added new members more quickly than any previous consortium.

From the Digital Twin Consortium's website: "The value of a digital twin cannot be overstated because of its ability to connect the physical and digital worlds providing real-time operational awareness of structures, machines, or products." Nicolas Mangon, Autodesk VP for AEC Business Strategy.

IoT versions of the application are in use in various sectors, including manufacturing and buildings, but the application is well suited for any IoT sector and is especially relevant to the IoT Edge when modeling is created using data from IoT edge devices.

Digital Twins is capturing the attention of IoT platform providers whose platforms include device management; such platforms have always included some form of asset visualization but real-time simulation adds another dimension.

Towards the Real Time Enterprise – Intelligent Systems

There are many pointers to the size and the importance of insightful, real-time information generated by the intelligent edge on an organisation's performance. The IoT market is predicted to encompass more than 75 billion IoT devices by 2025 (source IDC). And Gartner reports that by 2022, 50% of enterprise-generated data will be created and processed outside a traditional data center or cloud, up from less than 10% in 2019.

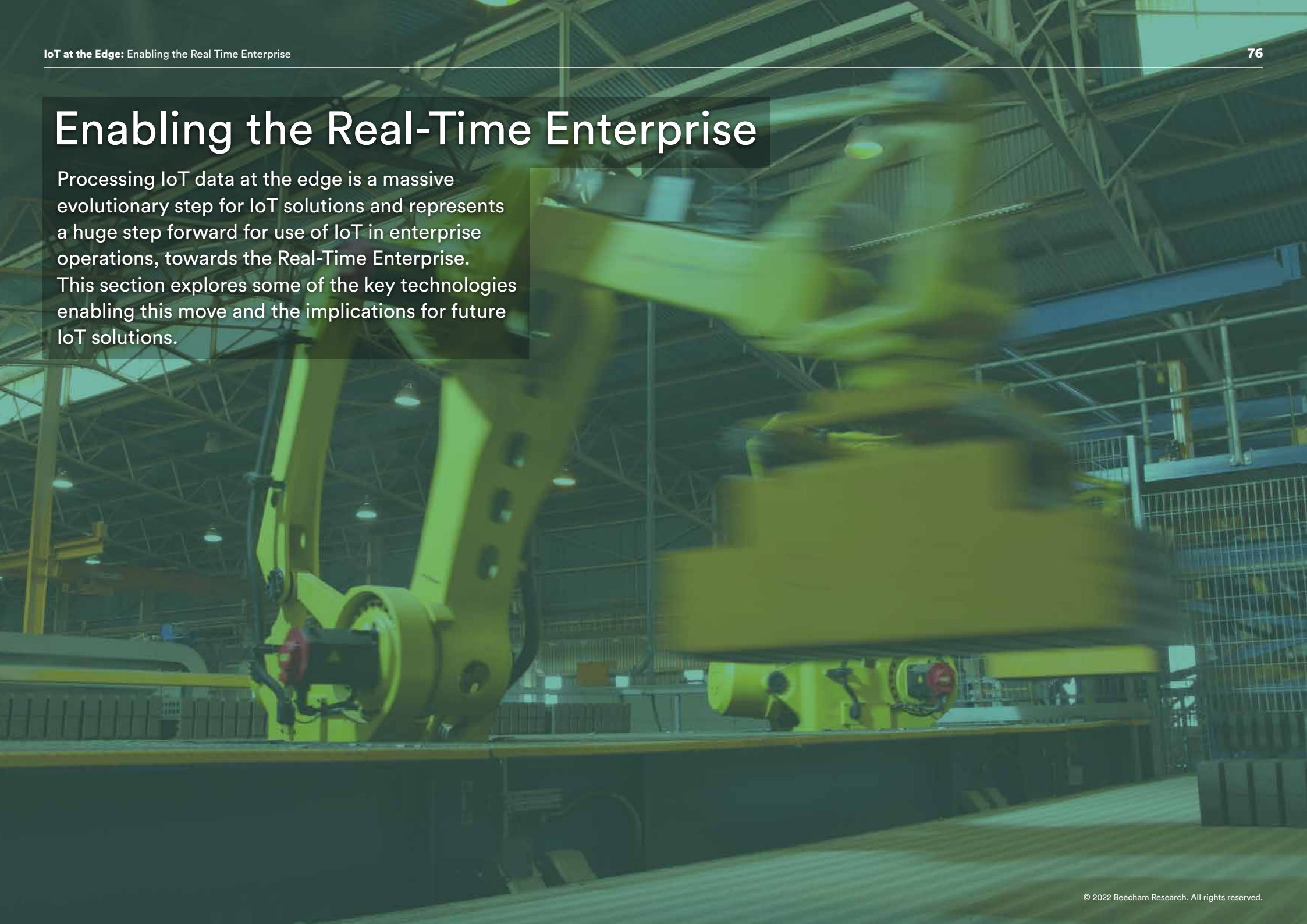
The intelligence in edge computing comes from the deployment of AI technology at the edge. Small, power efficient and cost-effective AI chipsets can be embedded in IoT devices and edge hardware such as the routers and gateways. This enables them to function as an intelligent network of small, local data centres, which in turn allows massive amounts of data to be processed locally, close to the source, thereby boosting the amount of real-time or near real-time information on which operational and management decisions can be based.

In a study conducted by the Boston Consulting Group and the MIT Sloan Management Review 75% of businesses said that AI, will allow them to move into new ventures and 83% believe that AI is a strategic priority for their business. In addition, AI is seen by 64% of CEOs as a way to lower overall OPEX. Pervasive AI can therefore realise immediate economic benefits as well as providing long-term differentiated value for the enterprise.

All of this indicates major changes within enterprises looking to embrace these real-time operation systems. **Wind River refers to this as enterprises moving towards becoming intelligent systems, covered in this report.**

Enabling the Real-Time Enterprise

Processing IoT data at the edge is a massive evolutionary step for IoT solutions and represents a huge step forward for use of IoT in enterprise operations, towards the Real-Time Enterprise. This section explores some of the key technologies enabling this move and the implications for future IoT solutions.



There is nothing new about the idea of a Real-Time Enterprise (RTE). Two decades ago the focus was on enterprises that fulfilled orders as soon as they came in – the on-demand enterprise. What is different this time is the increased role of IoT in business activities, enabled by edge computing's ability to process and analyse IoT data close to the source and generate real-time information and intelligence. That ability has resulted in IoT's core functionality transitioning from monitoring and reporting, a role that was traditionally performed in the cloud, to local control and automation. With IoT data processed at the edge, enterprises can now employ outcome-driven solutions that operate in real-time environments that comprise intelligent devices, intelligent systems and intelligent networks.

IT-OT convergence is a related development. It involves the integration of Information Technology systems (which handle enterprise-wide computing and data processing, usually with batch update) and Operational Technology systems (which manage and control industrial operations in near real time). The blending of IT and OT allows organisations to make better use throughout the enterprise of data generated by IoT devices and edge computing. This process is being enabled by deploying a new generation of operational technologies that operate alongside existing enterprise IT systems.

Processing data close to the source is a strong benefit, analysing the results and gaining valuable insights in real-time can be a challenge. The current hype surrounding AI is confusing and this can make it difficult to align the benefits of real-time intelligence with business goals and objectives.

Developing the Business Case

Edge computing has advanced the performance and functionality of business applications. For example, it enables a wind farm to analyse shifts in wind direction in real time and tilt the angle of its blades to capture more power. In the oil and gas industry, pressure and humidity sensors in pipelines need to be closely monitored. Real-time operation is also influencing customer experiences. Today's economy is predicated on the ability to provide customers with what they want, when and where they want it. To do this, companies will increasingly need to provide information to customers in near real-time.

There are numerous applications that are either enabled or enhanced by the application of edge processing to business processes and operations. Streaming transaction data can be monitored to detect anomalies that signal fraud in real-time and stop fraudulent transactions. A UK police force is using the technology to improve outcomes on crime, reduce harm, and identify vulnerabilities using existing resources. Real-time shipment visibility systems lead directly to better customer service, which is a significant competitive differentiator. A US company found that each customer-generated "the truck is late" call cost them $600 to $700.

Edge computing is also growing in importance in IoT environments where there may be intermittent access to connectivity, low tolerance for network latency, and/or high security demands.

In addition there is a generic business case. By radically reducing the elapsed time in business processes, the RTE can sense and respond quickly to events that affect its business. And enterprises are being challenged by the ever-growing volume of data and the need to process it quickly. IDC has estimated that 59ZB (Zettabytes) of data was created in 2020. The issue is the time taken to turn that data into actionable information.

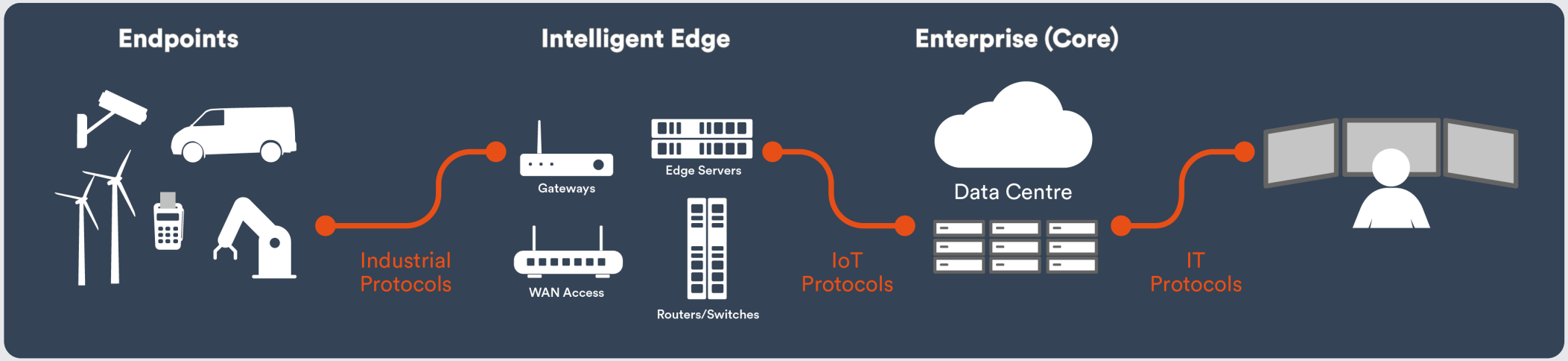
The Intelligent Edge

IoT is predicated on the ability to capture parameter and event data and process it into valuable, insightful information. Transforming information into intelligence is increasingly coming from the deployment of Machine Learning and Artificial Intelligence technologies at the edge as well as in the cloud. Small, power-efficient and cost-effective AI chipsets can now be embedded in IoT edge hardware. This enables them to function as an intelligent network of small, local data centres, which in turn allows large amounts of data to be processed locally, thereby boosting the amount of information on which operational and management decisions can be based.

Advances in chipset technology have boosted the computing resources of the devices deployed at the edge. This has enabled intelligent edge computing to perform data analysis tasks that were previously undertaken at a central facility such as the cloud. For example, if a security breach is discovered, the ability to turn off a feature in real time becomes a mission-critical requirement. In addition, edge computing enables companies to carry out authentication tasks closer to end users, which is inherently more secure.

The intelligent edge employs connected devices that have the ability to gather, receive and send information, embed intelligence and connectivity, set up applications, and automate processes. It is a development that highlights the economic and social potential of IoT solutions. The ability to deploy massive numbers of intelligent systems that can compute, sense, learn and adjust in low latency time is enabling numerous new applications right across the business spectrum.

Figure 4.1 *Advances in chipset technology has enabled intelligence, the processing and analysis of raw IoT data, to be provided in near real time at the edge of the network.*



The edge-to-cloud model

IThe intelligence shift towards the edge of the network enables the centralised cloud to be used for computationally intensive tasks, for example analysing bigger data sets from a wider range of sources and employing advanced analytics to gain information on trend s Edge and cloud computing therefore perform complementary, symbiotic roles. Edge devices only provide the results from data that was processed locally, after which it is normally discarded. Only useful, post-processed information is sent to the cloud and stored. The cloud can be used to blend real-time IoT information with up-to-date information from enterprise applications such as CRM and ERP.

The edge continuum

As outlined in Section 3 Market Analysis of this report, the increasingly important role that the edge plays in the IoT environment is reflected in the number of terms that are employed. They include far edge and near edge; thin edge, thick edge plus the network edge; and then there is fog computing, which acts as a mediator between the edge and the cloud. The term edge continuum is used to indicate the need to put the requisite compute resources at the optimal processing points; from cloud and private data centers to edge systems and devices.

The far edge is the infrastructure deployed in a location farthest from the cloud data centers and closest to the users. The near edge is the infrastructure deployed between the far edge and the cloud data centers.

In thin edge computing, less processing occurs at the point of sensor data collection. Thick edge computing involves a distributed approach. The IoT sensors and devices are connected to network nodes running edge applications close to where the data is collected, i.e. the network edge.

Fog computing and edge computing are both about processing data closer to the source—a significant difference concerns the place where processing occurs. Fog computing is an extension of cloud computing. It acts as a mediator between the edge and the cloud.

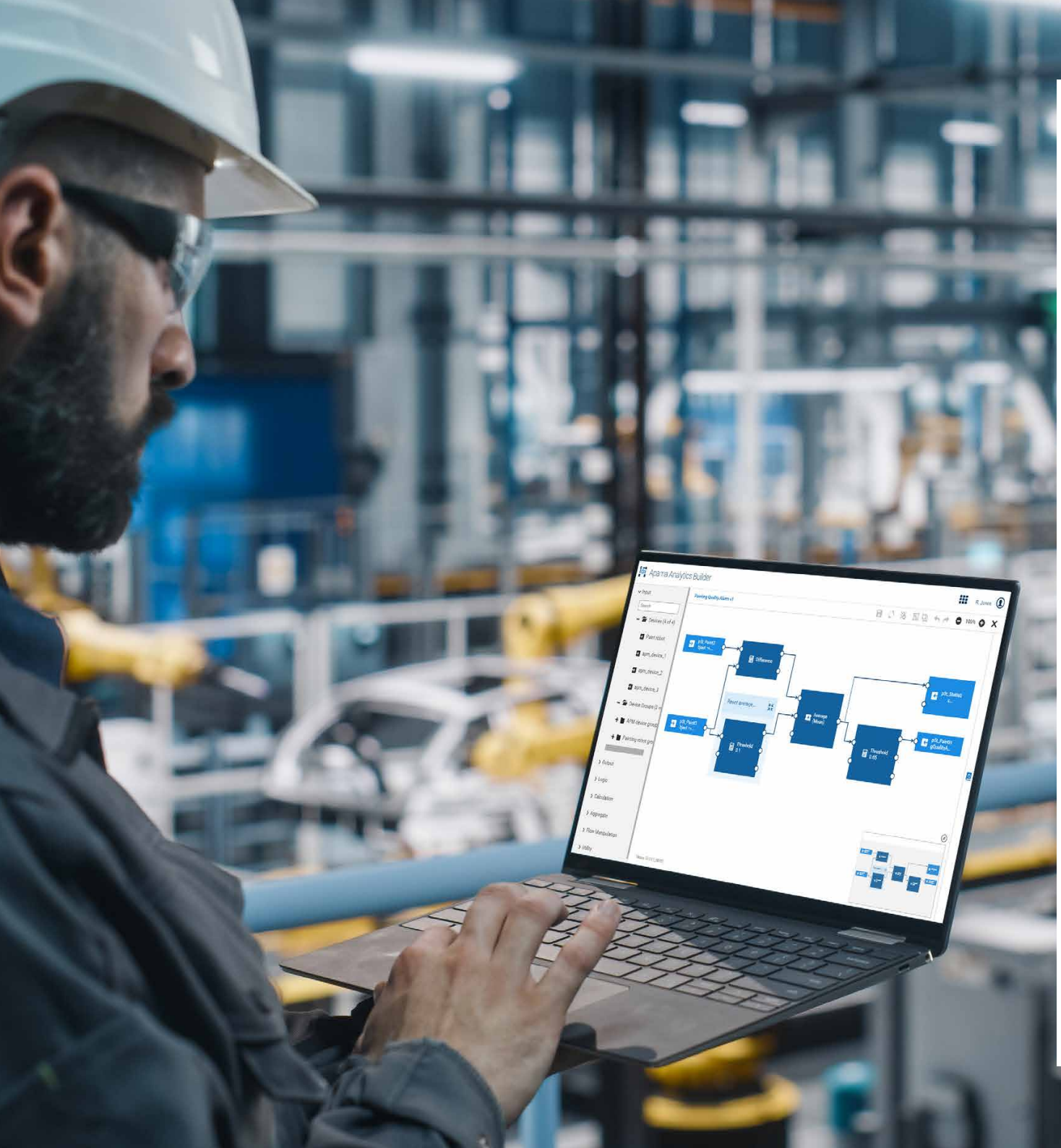
Cloud native edge computing

A cloud-native architecture employs microservices, which are small, independently deployable, loosely coupled modules. These are grouped together typically for well-defined tasks in small software packages called containers. They are building blocks that can be exchanged when larger scale deployments are required and when applications need to be modified in line with changes in the market and the organisation's requirements.

In contrast, today's IoT applications are typically based on a monolithic architecture. As such they are self-contained, proprietary developments and difficult to scale. Physical access and security are challenging, and edge devices are not standardised or interchangeable like servers in a data centre. In order to address these concerns and continue to evolve and scale easily, edge IoT applications are migrating to a cloud-native architecture that employs similar microservices to those of cloud-centric applications. This makes it much easier to enable orchestration between edge and cloud in a way that adapts to different application requirements.

Cloud intelligence

While much of the focus in the media is on intelligence at the edge, the symbiotic relationship with the cloud is equally important. For example, Microsoft Azure IoT Edge is a fully managed service that enables artificial intelligence, Azure and third-party services, plus customer business logic to run on IoT edge devices via standard containers. By moving certain workloads to the edge of the network, devices spend less time



DÜRR empowers factory operators to improve operational efficiencies themselves. **Do you?**

By using self-service industrial analytics at the edge, Dürr's automotive customers increased quality while decreasing paint consumption by 50%.

Discover how you can leverage leading industrial IoT edge computing to serve customers better at **softwareag.com/iot-edge-computing**

software AG

communicating with the cloud, react more quickly to local changes, and operate reliably even in extended offline periods. The computing and communications resources of the cloud enables billions of devices to be connected, monitored and controlled.

AWS has a similar offer. The company highlights the ability of the cloud to spin up resources as needed. They range from infrastructure services, such as compute, storage, and databases, through to IoT, machine learning, data lakes and analytics. These services can be employed in a matter of minutes, enhancing the ability to experiment and test new ideas. In addition, with cloud computing, there is no need to over-provision resources up front to handle peak levels of business activity. Resources can be scaled up or down in line with changing business requirements.

Towards intelligent systems

Intelligent system definitions vary, but the functionality is clear. An intelligent system is a machine with an embedded, computing facility that has the capacity to gather and analyse data and communicate with other systems. Other criteria for intelligent systems include the capacity to learn from a wide range of inputs including experience, security and connectivity, to adapt according to current data and have the capacity for remote monitoring and management.

As noted earlier, the intelligent edge focuses on intelligent devices. Intelligent systems involve interconnected populations of these devices as well as networks and other types of larger systems.

The ideas and practices behind intelligent systems are at the same stage digital transformation was in by 2015 and this represent a significant move forward in the development of IoT platforms. But the growth of intelligent systems at the edge is likely to be faster and deeper, because as enterprises become increasingly software driven, intelligent systems are expected to become the norm for such systems.

Products will increasingly need to be intelligent to be useful in operational terms, not just intelligent as a value-added experience. Functionality will typically include adaptability, self-optimisation based upon a goal or goals, the ability for performing self- diagnostics and self-maintenance, as well as the ability to learn and reason.

See the approach of Wind River to intelligent systems in this report. The company views intelligent systems as representing the next wave of the digital machine economy, a wave that is set to develop over the next five years.

Useful Web sites:
The Cloud Native Computing Foundation (www.cncf.io/) serves as the vendor-neutral home for many of the fastest-growing open-source projects. The foundation defines cloud native as technologies that empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds.

thin-edge.io (https://thin-edge.io/) is the first open-source, cloud-agnostic IoT framework designed for resource constrained edge devices. Its ready-to-use modular components can be easily deployed on a wide range of PLCs, protocol gateways and devices using Linux-based operating systems. See Software AG detail on thin-edge.io in this report.

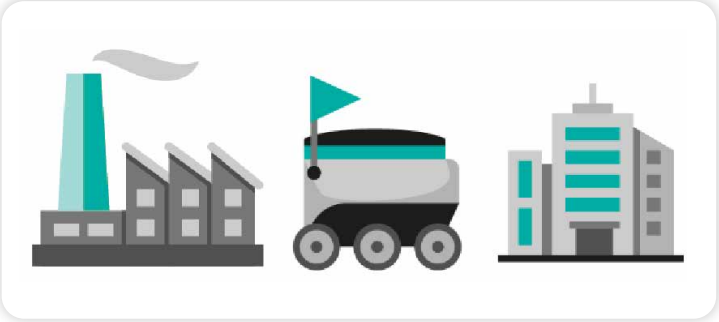
Edge Computing Association (https://edgecomputingassociation.com/) is an edge computing news resource and information forum on topics such as edge application architectures and hybrid peer-to-peer and blockchain technologies.

WNDRVR

Using an Intelligent System for Autonomous Transport

Beta Autonomous Vehicles

Autonomous delivery vehicles to work across a complex manufacturing campus environment (people, moving items) and across public roads.



Initial Assumptions Need Testing

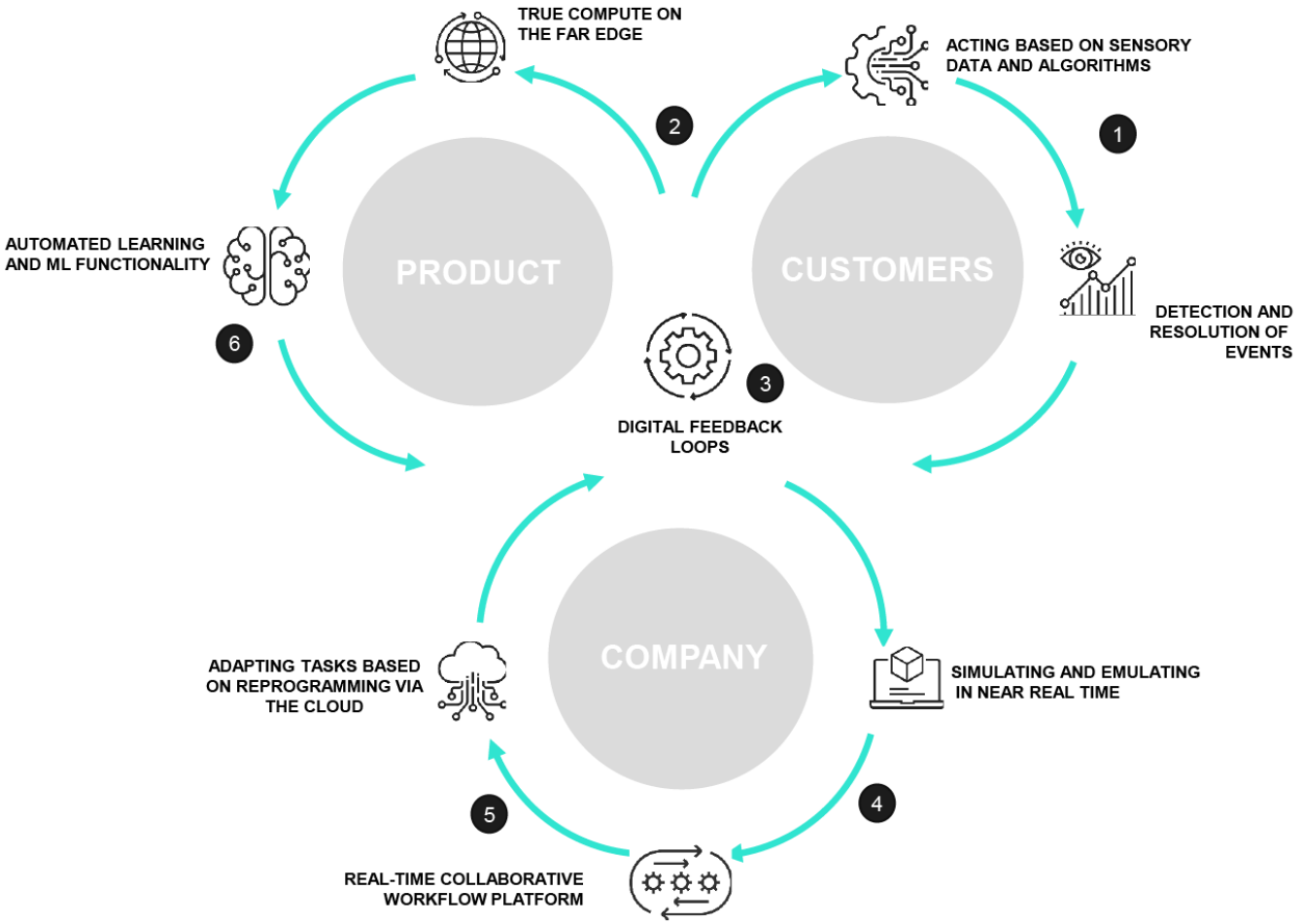
The vehicles start encountering unpredicted elements (people, other vehicles on campus, and wear and tear on key components) that take them out of service [1].

Intelligence Infused into System

Digital feedback loops [3] from sensors on the vehicles show where the weight is too much, and simulations [4] with new data show which components need to be replaced more often. Vehicle routes are also altered to reduce heavy loads late in the delivery cycles, with teams across development and operations [5].

Digital Feedback Loops

Repair times are reduced, and new vehicles are redesigned with rules for working in crowded environments (re-routing preferences) and load management [6].



thin-edge.io – The Open Edge Framework for Lightweight IoT Devices

Industrial equipment manufacturers face several challenges when creating connected products. Tackling these challenges has resulted in 58% of embedded projects being completed late, regardless of advances in development tooling and methodology (EE Times). Connected product manufacturers need: secure cloud and hardware agnostic connectivity; robust device management; and this software to be efficient on resource constrained devices.

Addressing the connectivity challenges is not made easier by the lack of standardization across the industry, forcing enterprises to make potentially irreversible decisions early in the design process that lock them to a single vendor. The open source thin-edge.io project provides a way for enterprises to retain their technology flexibility.

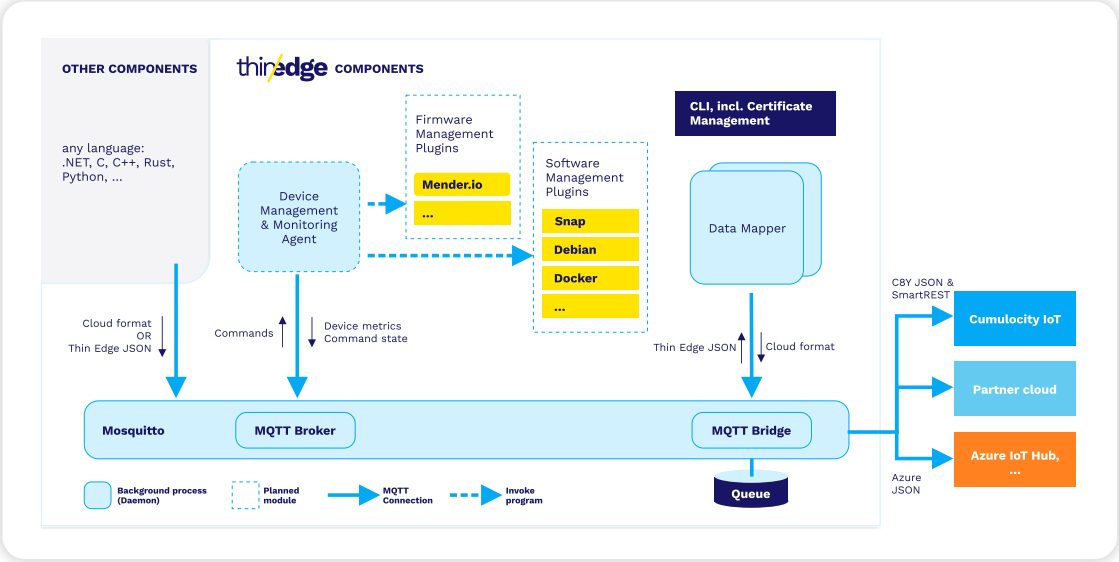
The modular architecture of thin-edge.io offers you the freedom to connect any IoT platform, use any programming language, adopt any message payload, deploy onto many hardware platforms, and manage any software artifact, such as Debian packages or Docker containers. The framework's plug-in mechanism also simplifies the integration with custom software. Comprehensive certificate management is built in with easy-to-use processes for both developers and operators. Its components can be deployed on a wide range of PLCs, protocol gateways and devices running Linux-based operating systems.

The software management agent in thin-edge.io allows flexible package management regardless of Linux distribution through receiving cloud agnostic commands and using plug-ins to perform the software installation and reporting independent from the software artifact type.

thin-edge.io has been developed in the reliable, efficient and secure Rust programming language and contains watchdog, device monitoring and remote access capabilities to assure the operational robustness essential for industrial embedded software.

Additional third-party community and commercial modules are already available for streaming analytics, machine learning, industrial protocol conversion, and industrial sensor applications.

thin-edge.io contributors include ifm, Software AG, Nexus Group, Inetum, ADAMOS, Brainboxes, Kunbus, and IPComm, each providing their own domain expertise.



Edge Compute Architecture

Figure 2 visualises the architecture's four main regions: the device region, the edge server/gateway region, the edge network or micro data center, and the enterprise hybrid multi-cloud region. The edge server not only connects all edge devices in a secure manner but also enables them to be managed.

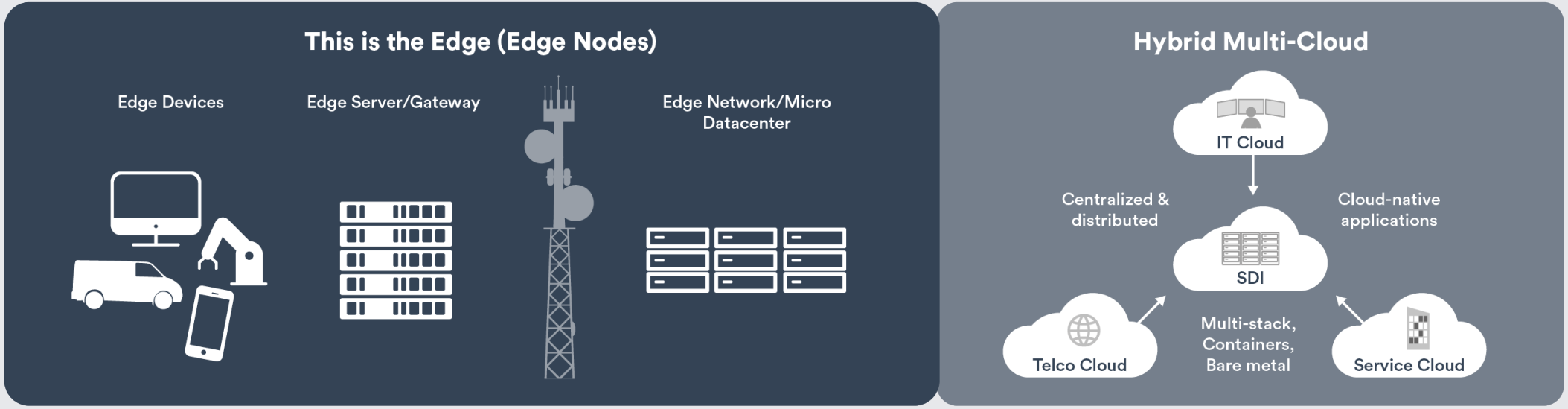
Devices. The edge devices are equipped to run analytics, apply AI rules, and even store some data locally to support operations at the edge. The devices may also have the resources to handle analysis without the involvement of the edge server or the enterprise region.

Edge server or gateway. Edge servers are used to deploy apps to the devices including more intensive AI processing. Thousands of edge servers maintain a pulse on the millions of devices. If something more than inferencing is needed, data from the devices is sent to the edge server for further analysis.

Edge network or micro data center. They reduce the distance that device data must travel, which decreases latency and bandwidth issues. This region also offers more analytical capabilities and more storage.

Enterprise hybrid multi-cloud. This region offers regular enterprise-level storage and management, device management, plus enterprise-level analytics and dashboards. It can be hosted in the cloud or in an on-premises data center.

Figure 4.2 *Gateways and servers aggregate the data, which is processed and analysed by a network of local micro data centres.*



Edge to Cloud Connectivity

The intelligent network – from 4G to 5G

5G networks are now being deployed, but coverage is not ubiquitous, which means that 4G/LTE is often still the mainstream communications service. 4G/LTE was a breakthrough development; it had an all-IP architecture and an Evolved Packet Core (EPC), a key component that can be virtualised, in other words enabled in software. 5G encompasses a much wider set of network developments that go well beyond a higher speed, lower latency version of 4G. Unfortunately, 5G has been over-hyped, particularly the radio infrastructure element, and this has obscured its importance as well as the role it is set to play in next generation, virtualized networks.

Coverage of 5G in the media has also been confusing. Early deployments were NSA (non-stand-alone), which did not bring any meaningful improvement in performance or functionality. 5G SA (stand-alone) will; it introduces three generic services: enhanced mobile broadband (eMBB), Ultra Reliable Low Latency Communication (URLLC), and massive Machine Type Communication (mMTC), as well as new functionalities such as network slicing. But deployment of these innovative services cannot start until the relevant 3GPP versions are finalised. For example, release 17, which focuses on the low-latency service for industrial IoT and is most closely associated with edge IoT, is expected during 2022, with services coming in 2023. However, it is worth recalling 4G/LTE took nearly a decade to evolve from 3G.

5G SA data infrastructure is a software-defined network that significantly raises the performance and capacity bar. With the mMTC generic services it can support up to one million devices per square kilometre and with eMBB it can transmit data at 10 gigabits per second. With URLLC, it offers very low latency which requires integration with the edge to deliver. With so many devices on the network, many operating in mission-critical systems, real-time visibility and advanced threat detection are required. The intelligent edge and the edge-to-cloud model are key components of this environment; both need to operate over an ultra-reliable, cost effective intelligent IoT network. Intelligence, enabled by AI, is needed to: Recognise connectivity gaps and act proactively to resolve them; identify ineffective connectivity patterns; and scan network and device behaviour for unusual, potentially harmful activity.

Use of LPWAN

As noted earlier, the effect of the intelligent edge is to reduce the amount of data sent to the cloud. It does not reduce the number of connections needed but it does increase the need for low data rate connections compared with high data rate. This lowers the overall connectivity cost compared with all data being sent to the cloud and processed centrally. Together with the 5G generic services, this is creating strong demand for Low Power Wide Area (LPWA) connectivity. **See Sierra Wireless connectivity featured in this report.**

LPWA connectivity features low power consumption (supporting years of battery life in connected devices) and a 5 to 15-km range. Device throughputs are a few hundred kilobits per second for cellular licensed spectrum such as LTE-M and NB-IoT, and less for unlicensed such as LoRa and Sigfox (**See Sony Semiconductors 'Cellular IoT Chipsets for Edge Devices' featured in this report**).

SONY

Cellular IoT Chipsets for Edge Devices

As IoT ecosystems evolve, end- to-end cloud solutions are designed to generate insights based on analysis of IoT devices' ambient data. In typical applications, the device gathers data from its environment and communicates it back to the cloud for analysis. In this configuration, there is a growing need to control the amount of data being transmitted to the cloud for analysis. The aim is to minimize communicated data by compressing pertinent data, improving cloud analysis performance and accuracy.

For cellular IoT applications this is even more important, given the data communication costs.

This leads to a significant amount of processing on the device side. In addition to the rigorous security and device management capabilities, which are fundamental to any IoT device, the device now needs to allocate precious compute power to analyzing, screening, and compressing the data it aggregates.

Sony's Altair ALT125x cellular IoT chipsets are built from the ground up to support edge device requirements, enabling much of the data processing to be executed on the device side. Their dedicated core for application development is detached from the modem operation. This ensures seamless operation of the modem for connectivity, where the application can take full advantage of a robust Cortex-M core, including tiny ML capabilities, enabling real-time analysis, and corresponding actions on the device side, reducing the data bandwidth to be communicated over the air, and improving data accuracy sent to the cloud for analysis.

The other major advantage of Sony's Altair ALT125x cellular IoT chipsets is the security architecture. Security in the IoT era is crucial. Sony's Altair chipsets integrate a multi-layered security architecture to enable highest level of security for applications running on the chipset. Featuring chip and device hacking-protection as well as a robust service access layer, Sony's Altair chipsets provide the most advanced hardware- and software-based tools to ensure end-to-end security. This gives our customers the ability to develop their application on the device side without worrying about the majority of security threats, as they are secured by design.

Learn more about our cellular IoT solutions
https://www.altair-semi.com/products/alt1250/
https://www.altair-semi.com/products/alt1255/

altair

The low data rates of LPWA are in line with the connectivity requirements of edge computing. When most of the data is processed at the edge and then discarded less real-time data needs to be transmitted to the cloud. LPWA parameters are also in line with the requirements of small, semi-autonomous thin edge devices that operate in distant locations.

Historically, enabling smaller devices to become thin edge devices has been a challenge. For example, if a problem occurs the device would "call for help," alerting online platforms that there are vibrations or humidity issues that cannot be managed locally. Moreover, the recent push to embed more intelligence into smaller devices such as AI-powered video cameras has raised the bar on securely connecting and maintaining these devices operating in live operational environments. In addition the fragmentation of hardware and software makes it difficult to employ a common IoT management platform.

This is where the **open source, cloud agnostic thin-edge.io initiative framework comes into play**. It offers simple, secure and reliable cloud connectivity to a wide range of cloud platforms. It is standards-based, container compatible and supported by a global developer community.

Private Networks and edge IoT

For a full briefing of cellular private networking, Beecham Research's report on 5G Private Networking is also available at www.5GPrivateNetworking.com.

As IoT has moved from 'nice-to-have' to an essential part of enterprise operations, 5G private networks (5GPNs) are now the biggest new opportunity for IoT deployment within the enterprise. Many of the reasons for this are common with the reasons for the huge growth of IoT at the edge.

5GPNs can take the growing need for cellular IoT in business operations to another level, in the process considerably enhancing the IoT offer. This includes innovative solutions that employ both licensed and unlicensed spectrum as well as combinations of public and private networks, potentially with seamless roaming between them.

When enterprises own their communications resource, IT management can take control of performance, security and resilience as required for local operations. They can determine user authorisation, how resources are employed and how traffic is prioritised. On a private network, data transfer is also secure; it remains on the company's premises. In addition, ownership allows these networks to be amortised; the financial model typically changes from OpEx to CapEx.

Embedded Connectivity and IoT SAFE

As noted in Section 3 Market Analysis of this report, embedded SIM (eSIM) was developed as a response to the problems of using the traditional plastic SIM cards in IoT devices. As also noted, the integrated SIM (iSIM) has been developed as an evolution of eSIM where the physical SIM sits inside a secure element within a System on Chip (SoC). This removes the physical component from the device circuit board, reduces power requirements significantly and also improves security compared with the eSIM solution. **See Kigen offering of iSIM in this report**

Associated with these SIM developments, a further GSMA initiative in addition to its work on eSIM/iSIM specifications is IoT SAFE (IoT SIM Applet for Secure End-to-End Communication). This initiative recommends that the industry should use the SIM as a hardware secure element or 'Root of Trust' to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted that the SIM is particularly well-suited

SONY

YOUR SMART CHOICE FOR CELLULAR IoT

- Leading provider of cellular IoT chipsets
- Globally certified
- Highly integrated LTE-M and NB-IoT chipsets
- Enabling long battery life
- Quality and lifetime partnership
- Security as core value – built in security, designed from the ground up

Learn more: www.altair-semi.com


Point of Sale


Healthcare


Smart Industry


Smart Cities


Smart Metering


Trackers and Telematics


Consumer Electronics


Agriculture

CONNECT FORWARD

Altair

for this purpose: it is one of the hardest of all identifiers to spoof, with advanced security and cryptographic features, is fully standardized, and has been deployed in huge numbers of devices for the past 30 years. Key characteristics of IoT SAFE include:

- Use of the SIM as a mini 'crypto-safe' inside the device to securely establish a TLS session with a corresponding application cloud/server
- Compatible with all SIM form factors (SIM, eSIM, iSIM)
- Provides a common API for the highly secure SIM to be used as a hardware 'Root of Trust' by IoT devices
- Helps solve the challenge of provisioning millions of IoT devices

The IoT SAFE applet runs on Java OS, which in turn runs on the iSIM OS.

Establishing Trust

Trust is essential to realise the full potential of the IoT. Digital security must be designed into IoT devices from the ground up and at all points in the ecosystem to prevent vulnerabilities in one part from jeopardising the security of the whole. This is easy to say but IoT ecosystems are complex. Machines and objects in virtually any industry can be connected and configured to send data over cellular networks to cloud applications and backends. The digital security risk is present at every step along the IoT journey, and there are growing numbers of hackers at national and international levels that seek to take advantage of a system's vulnerability. Unfortunately, diverse data types and computing power among IoT devices mean there is no 'one size fits all' cybersecurity solution that can protect every IoT deployment.

The first step for any IoT business is to undergo a thorough security risk assessment that examines vulnerabilities in devices and network systems and user and customer backend systems. Risk must be mitigated for the entire IoT lifecycle of the deployment, especially as it scales and expands geographically.

Root of Trust is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as verifying digital signatures, solutions will normally include a hardened hardware module. This is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

In IoT a root of trust consists of identity and cryptographic keys rooted in the hardware of a device. It establishes a unique, immutable and unclonable identity to authorize a device in the IoT network. Since the root key is generated internally and never stored, no sensitive data is visible anywhere in the supply chain.

PSA is an architecture-agnostic framework designed to help companies secure their devices from the ground up and is available free of charge. The four-phase approach helps analyse use cases, architect systems, implement the solution, and then certify that everything is working as expected.

PSA Certified is the security certification scheme for IoT hardware, software and devices that was created by seven stakeholder companies as part of a global partnership (See PSA-Certified details in this report).

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 4.4 *PSA-RoT on-chip security*

psacertified™

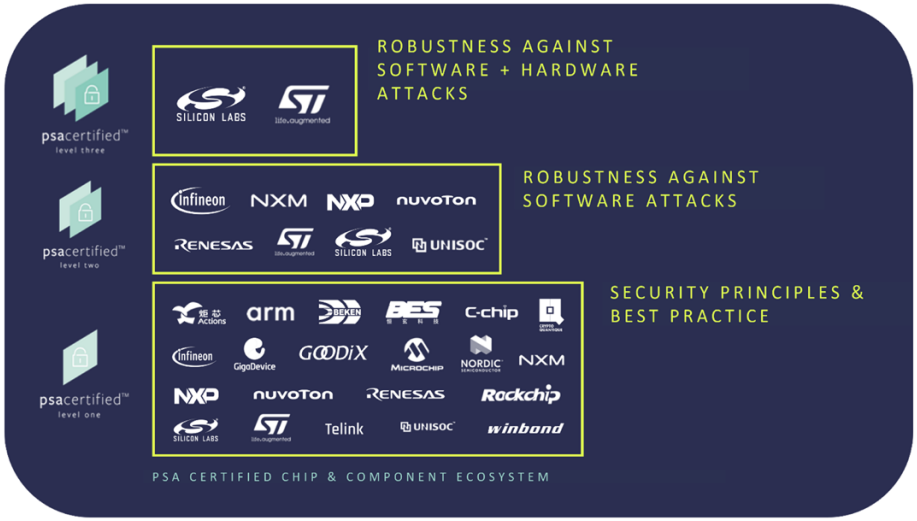
System software vendors and device manufacturers can then build on the certified PSA-RoT and certify their products based on these implementations. This deepens the understanding of the RoT within the technology ecosystem and then creates a value chain based on a standardized and trusted foundation.

> ***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 4.5 *PSA Certified chip and component ecosystem*



Data Analytics

The intelligence in edge computing comes from the deployment of advanced data analytics technology at the edge. The computing resources that perform analytics tasks provide data processing capabilities at the speeds needed to identify and route critical data in mission critical applications. Advances in edge technology will enable businesses to run more powerful and accurate models on smaller edge hardware, thereby enabling data analytics to be deployed more rapidly and cost-effectively. In addition edge computing's distributed nodes can handle complex computation tasks without exchanging data with the cloud.

Empowering this edge hardware with Machine Learning (ML) and Artificial Intelligence (AI) boosts their ability to process and analyse data, a development enabling the creation of innovative applications such as machine vision and voice recognition. Until recently it would have been impossible to run AI locally as the hardware size and cost would have been prohibitive.

Machine Learning is the science of getting computers to "learn" without being explicitly programmed. It enables decisions to be made with minimal human intervention. ML makes assumptions, learns and provides predictions at a scale and level of detail that would be impossible for humans. The algorithms run on edge platforms.

ML is a sub-set of AI, which is a broad concept that enables machines to do "smart" things and act intelligently. It works by combining large amounts of data with fast, iterative processing and intelligent algorithms, allowing the software to learn automatically from patterns or features in the data.

There are many benefits to edge AI. It improves the reliability of the process by reducing service interruptions associated with transferring data from the cloud to the point of delivery. Edge technology also largely eliminates privacy or compliance concerns by allowing data to be more securely processed or stored at the edge, rather than in the cloud.

ML and AI platforms

Machine Learning platforms provide users with tools to build, deploy, and monitor ML algorithms. They combine the intelligent, decision-making algorithms with data, thereby enabling developers to create a business solution. Some platforms offer prebuilt algorithms and simplistic workflows with such features as drag-and-drop modelling and visual interfaces that connect the requisite data to the end solution. The algorithms will typically include image recognition, natural language processing and voice recognition.

AI software platforms provide the functionality to analyse, organise, access, and provide advisory services based on a range of both structured and unstructured information. These platforms facilitate the development of intelligent, advisory, and AI applications, including intelligent assistants that may mimic human cognitive abilities. The technology components of AI software platforms include: Text analytics, rich media analytics, tagging, searching, machine learning, categorization, clustering, hypothesis generation, question visualization, filtering, alerting, and navigation.

SIERRA WIRELESS

Managed IoT Connectivity Services

One IoT Connectivity Partner

One Global SIM

One Management Platform

Purpose built IoT Connectivity solutions with one point of accountability to ensure your business-critical assets are “always on”.

See (Section in this report) for more details

https://www.sierrawireless.com/products-and-solutions/iot-connectivity/

AI Chipsets

AI chipsets are specialised silicon hardware designed for specific tasks defined in hardware. They run the algorithms and thereby realise the high speeds and efficiencies necessary for large-scale AI-specific calculations. These chipsets are also known as AI accelerators.

The performance of edge and cloud computing are enhanced by different AI chipsets. A cloud chipset generally has higher computational power, higher power consumption, as well as a larger physical footprint, and is therefore relatively more expensive. Edge AI chipsets are smaller, more power efficient and less expensive – features that enable them to be embedded in IoT hardware as well as cameras, connected healthcare, smart retail, robots, and other IoT-enabled products.

Standardisation at the Edge

The Multi-access Edge Computing (MEC) initiative is an Industry Specification Group (ISG) within ETSI (European Telecommunication Standards Institute). Its purpose is to create a standardized, open environment which will allow the efficient and seamless integration of applications from vendors, service providers, and third-parties across multi-vendor Multi-access Edge Computing platforms. It formalises the creation of the small, local data centres outlined earlier. In MEC parlance they are local, cloud-based micro data centres (aka cloudlets).

This is a significant development since edge compute may involve processing and analysing data from different sources. In the absence of standards this is conducted in the cloud, where there is more standardisation, but it needs to be done at the edge in order to create an open market. This work is closely linked with 3GPP's specifications for 5G networks since 5G and edge computing are inextricably linked, in particular for the delivery of low latency connectivity. Further details on this can be found in 3GPP's white paper 'MEC in 5G networks'.

Digital Twins

Digital Twins is a software application that can model and/or simulate a single device, large deployments of devices, processes and systems, or even workers' tasks, by creating a digital counterpart.

The application originated with NASA Apollo missions and has long been associated with CADCAM, product design and engineering, and product lifecycle, but is moving towards integration with IoT platforms.

There is no universal definition and digital twins are still evolving. Many varieties are offered by vendors but digital twins are presently in use in

Industrial IoT (IIoT) environments and increasingly in other sectors such as smart buildings and healthcare, while some IoT platforms with device management features are expanding or enhancing those features with a digital twin. Capabilities for some digital twin offerings read like device management capabilities for IoT platforms.

IoT digital twin applications are tied to the IoT edge as they rely on device data. This will include metadata (including device details such as serial number, model year, make, firmware version, etc.) when a device is activated, authenticated, and registered on an IoT platform, and state data, which is dynamic and typically real-time in nature and can be used for monitoring, control, and maintenance with AI, Machine Learning, and predictive data analytics.

As Digital Twins can be used to model or simulate either products or processes, some use cases such as product design and optimization will benefit engineering groups. Product usage, operations intelligence, predictive monitoring for maintenance, and remote service will be familiar to IoT users. As Augmented Reality (AR) and Virtual Reality (VR) user interfaces become untethered thanks to improved connectivity options, digital twins can also be used by workers, including remote field workers – not just those within a facility, to enhance productivity.

Unlike an IoT platform, digital twins can be used throughout a product's lifecycle from design through to development and deployment, but in time digital twins may become IoT platform modules or serve as the core of new IoT platforms. Microsoft already markets its Azure Digital Twins as an IoT platform that can be integrated with Azure IoT hub. AWS recently announced its IoT Twin Maker in "preview" mode. It will offer 3D visualization and connect with other graphic applications. Integration with various IoT offerings is likely.

Digital Twin Standards

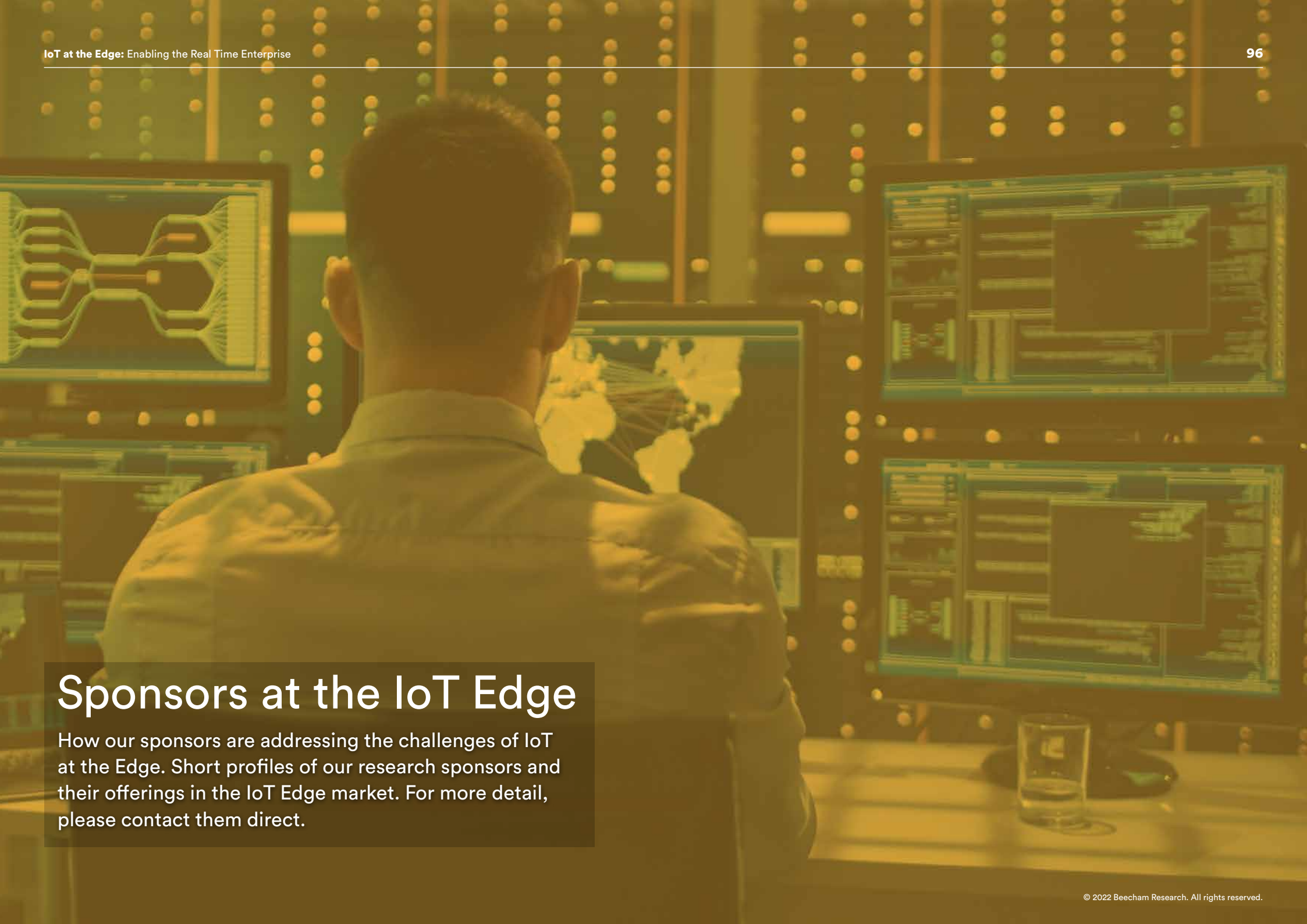
The use of digital twins is growing rapidly, but with so many versions there is a lack of standards that would hinder market growth if it continued.

At least eight different groups are working to create standards, including the Digital Twins Consortium (DTC), founded in May, 2020. DTC is managed by the Object Management Group (OMG) and growing faster than any previous OMG consortium. DTC has liaisoned with the other seven groups and had nearly 150 members only four months after its founding.

Membership is open to any business, organization or entity with an interest in digital twins. DTC's Use Case Reference Library, a member contributed collection of real-world use cases, is expected to be publicly available soon.

Summary

IoT hardware comprises sensors, modems, devices, SIMs, routers and gateways. IoT related software generates actional information on parameters and events and the addition of machine learning and artificial intelligence at the edge provides real-time intelligence. Informed decisions can now be taken locally, automatically in some cases. Less data needs to be sent to the cloud; real-time data that is sent can be blended with data generated by mainstream business applications such as CRM and ERP. Intelligence has become pervasive; enterprises are increasingly operating in real-time environments that are overlayed with security mechanisms.



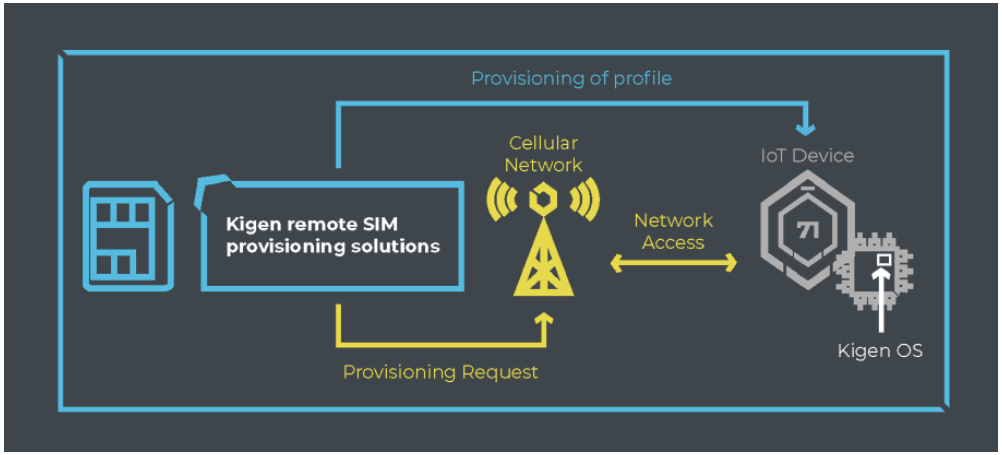
Sponsors at the IoT Edge

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

WEBSITE

Kigen

Integrating security for limitless opportunities in enterprise edge.
With the ever-accelerating growth of the IoT, more devices than ever will require scalable connectivity. Kigen's SIM, eSIM and integrated SIM solutions help chipset makers, device makers and enterprises to simplify manufacture, overcome cost challenges and build secure foundations for IoT edge devices. Integrating the SIM functionality into the application processor SoC of the device, enables users to active, manage and update edge devices. Greater integration of standards-compliant security allows to meet the lower size and power requirements, attractive for edge devices with machine learning and AI capabilities.



Enabling global, scalable and secure IoT connectivity
The Kigen family of products is a comprehensive suite of technologies that enables global, scalable and secure cellular IoT connectivity, whilst maintaining the industry recognized levels of security.

- Connectivity out-of-the-box
- Flexibility for addressing many form factors for different IoT devices
- Highest level of security and quality of service

Kigen SIM Solutions

OS products

SIM OS | eSIM OS | iSIM OS

Compact code

Implementation flexibility

Can be ported to multiple hardware form factors

GSMA compliant

Supports a variety of eSIM grades (automotive, industrial and consumer)

SIM management solutions

Remote SIM provisioning solution | OTA server | Server hosting | Server sandbox

Built on state-of-the-art open-source frameworks and technologies Seamless integration with a broad range of MNO and flagship IoT provider platforms

SAS-SM certified

Tools and services

Support & maintenance | Tools & applets | Profile development and consulting

Tailored

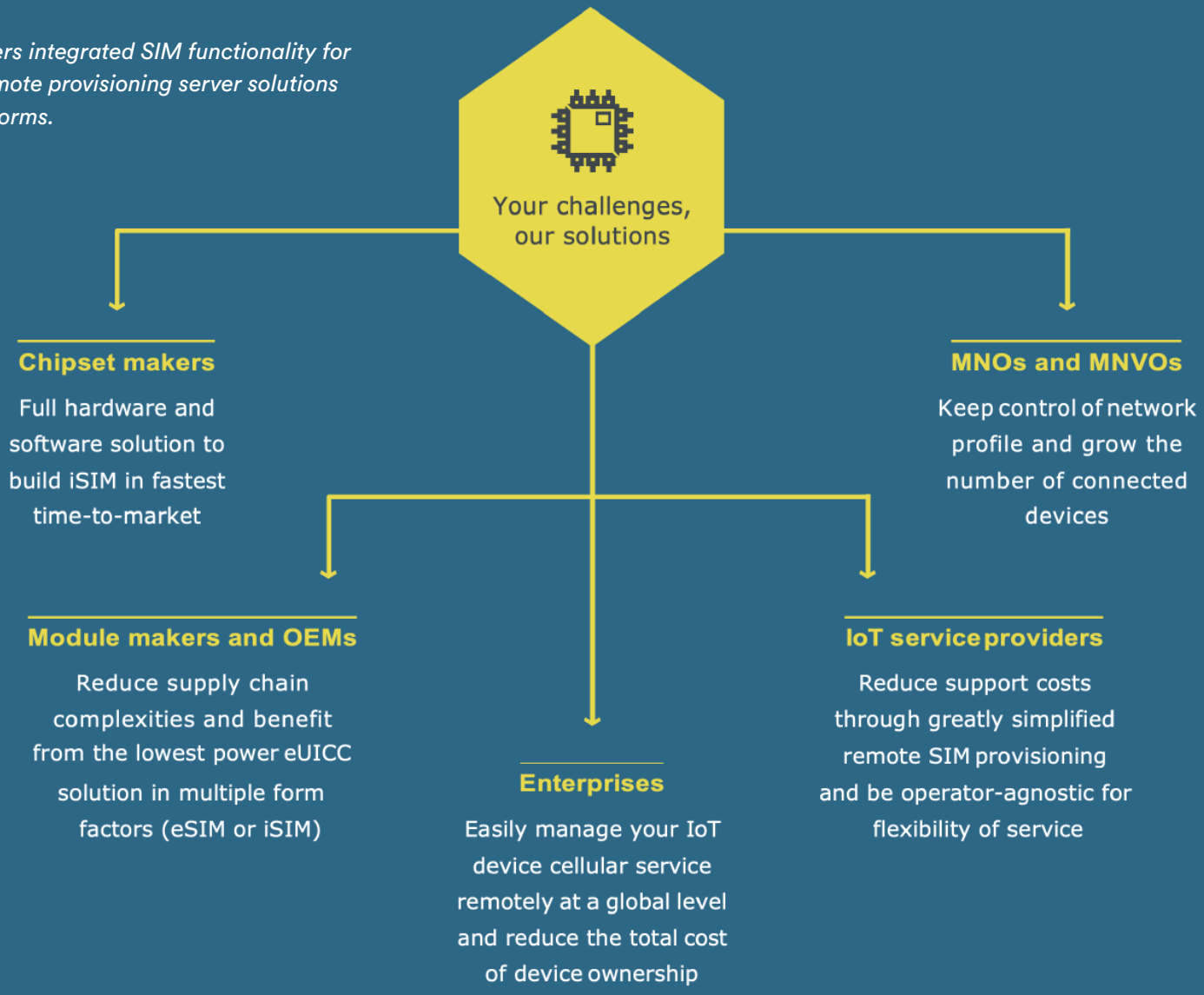
Flexible

Delivered in-house

WEBSITE

Kigen

Figure 2. *The Kigen family offers integrated SIM functionality for IoT SoC design and flexible remote provisioning server solutions for OEMs, MNOs and IoT platforms.*



WEBSITE

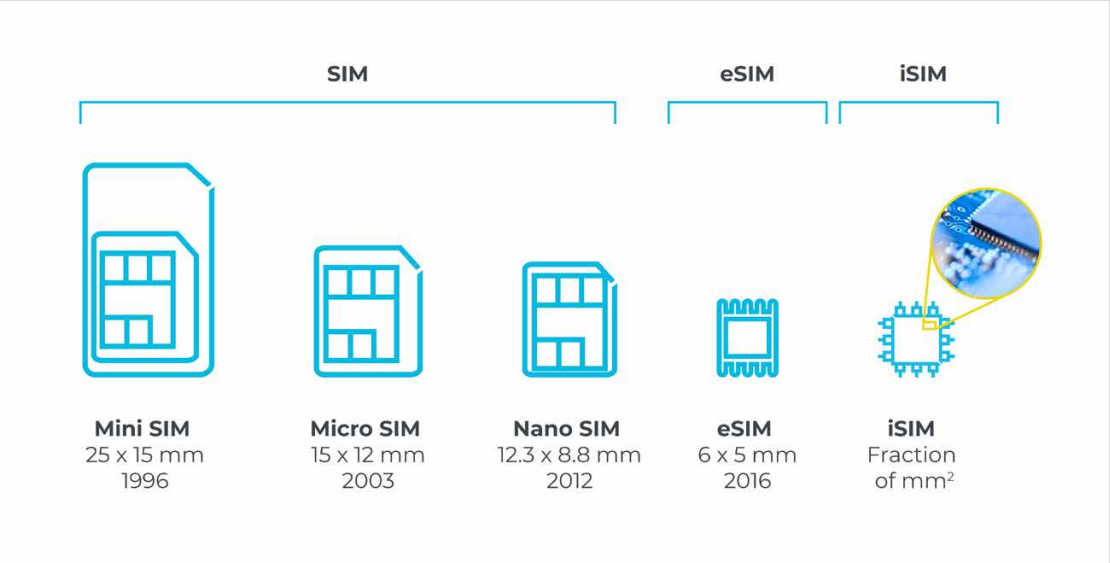
Kigen

iSIM shapes the enterprise edge of the future

We recognized that although the eSIM addresses many traditional SIM challenges, it could benefit from further optimizations while retaining SIM security. iSIM is a fraction of a millimeter in size because it is integrated into the same chip as the processor as part of the manufacturing process. This enables:

- Significant reduction in silicon footprint
- Lower power consumption
- Reduced device cost
- Longer device life due to reduced component count
- Elimination of the component sourcing and manufacturing practices associated with separate SIMs

How can Kigen's security solutions support your enterprise edge needs? Find out more on https://kigen.com and get in touch.



WEBSITE

psacertified™

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 witha 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.

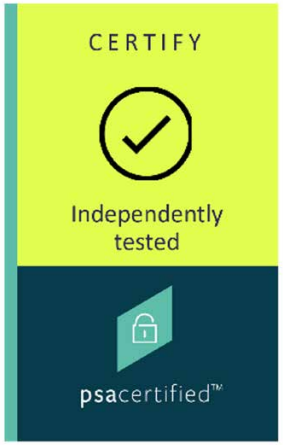
Methodically Created and Independently Tested

The certification program was created methodically by industry-leading experts. Independent and unbiased assesment 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:



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

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

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

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.

WEBSITE

psacertified™

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

SIERRA WIRELESS®

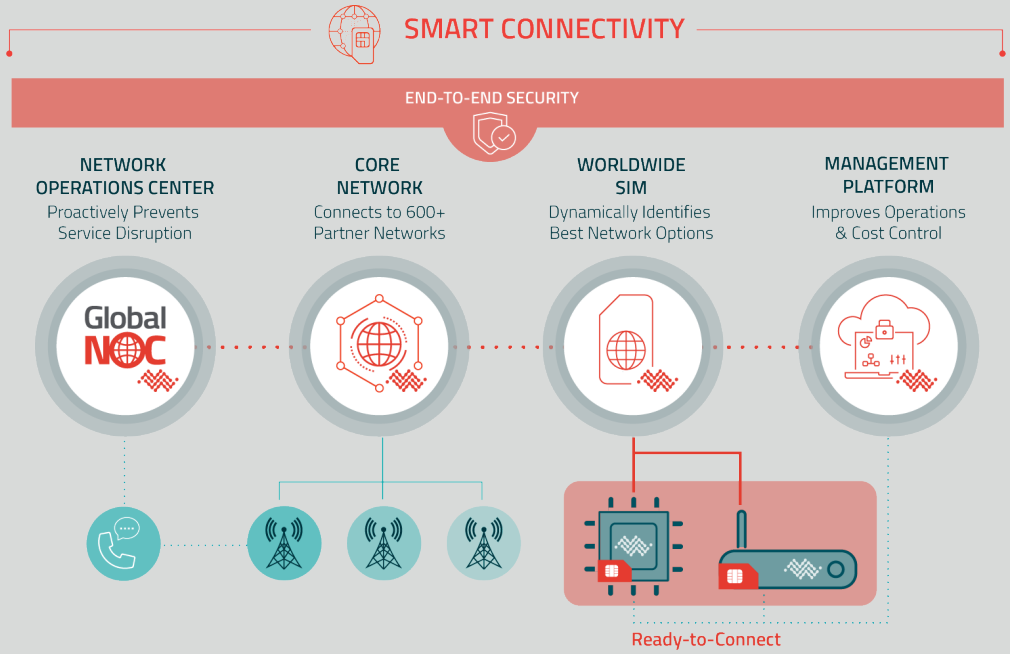
Sierra Wireless Smart Connectivity service is designed to simplify and augment global IoT deployments. This service makes it easy to maintain a secure and reliable connection to both fixed and mobile assets anywhere in the world. It also provides multiple redundant routes to 600+ partner networks in order to eliminate local coverage gaps. Instant access to the service is enabled by Ready-to-Connect modules, gateways and routers. eSIMs that are pre-integrated inside Ready-to-Connect devices can be activated over-the-air, thereby eliminating individual device provisioning. If there is an outage, the eSIM automatically selects the next strongest, available network in the area.

As shown in Figure 1, Smart Connectivity provides secure and resilient global coverage and includes the following key components:

- Network operations center – Proactively prevents service disruption with 24/7/365 monitoring of our geo-redundant core network.
- Core network – Delivers secure redundant routes to multiple networks in every country to eliminate local coverage gaps.
- Worldwide SIM – Dynamically identifies the best network options in real-time with access to 600+ partner networks in 190+ countries.
- Management Platform – Improves operations and cost controls by providing a consistent experience and unified view of Sierra Wireless SIMs and devices.

The Sierra Wireless SIM has a patented embedded agent that dynamically identifies the best network options available in real-time with multiple routes to multiple networks in every country. This multi-IMSI, multi-network feature is referred to as Smart Connectivity Advanced.

Figure 1. *Sierra Wireless Smart Connectivity service elements, with Ready-to-Connect*



WEBSITE

Ready-to-Connect: Plug and Play Solution with fully integrated cellular devices

In addition to the components above, Ready-to-Connect offers a plug and play solution. It comes with pre-integrated, pre-tested and pre-secured components, removing many of the difficulties associated with ensuring interoperability and security. The whole is designed to reduce complexity at every point in the IoT stack - from device to Cloud to central IT system. Of all the steps involved in an IoT deployment, the task of integrating all the components of the solution is often the most complex and time consuming.

Further, the 'Ready-to-Connect' modules, gateways and routers provide instant access to the Smart Connectivity service, thereby simplifying IoT development. They enable a tightly integrated and secure data stream to the Cloud, while eSIMs pre-integrated inside the Ready-to-Connect devices can be activated over-the-air anytime, anywhere, reducing the need for individual device provisioning and reducing gaps where errors can arise.

Wireless Gateways consist of dedicated hardware appliances or software programs and serve as a connection point between the Cloud server/application and the devices and/or sensors. Sierra Wireless' Gateways guarantee a very secure connectivity. They pre-process the data package before sending it to the Cloud; in addition to collecting the desired patient data, they collect data on device and machine status and location.

Secure from the Device to the Cloud

To address device security, the concealed eSIMs in the Ready-to-Connect modules prevent SIM tampering or theft, along with the latest encryption technologies in the device, network, and cloud to create layers of protection for the deployment.

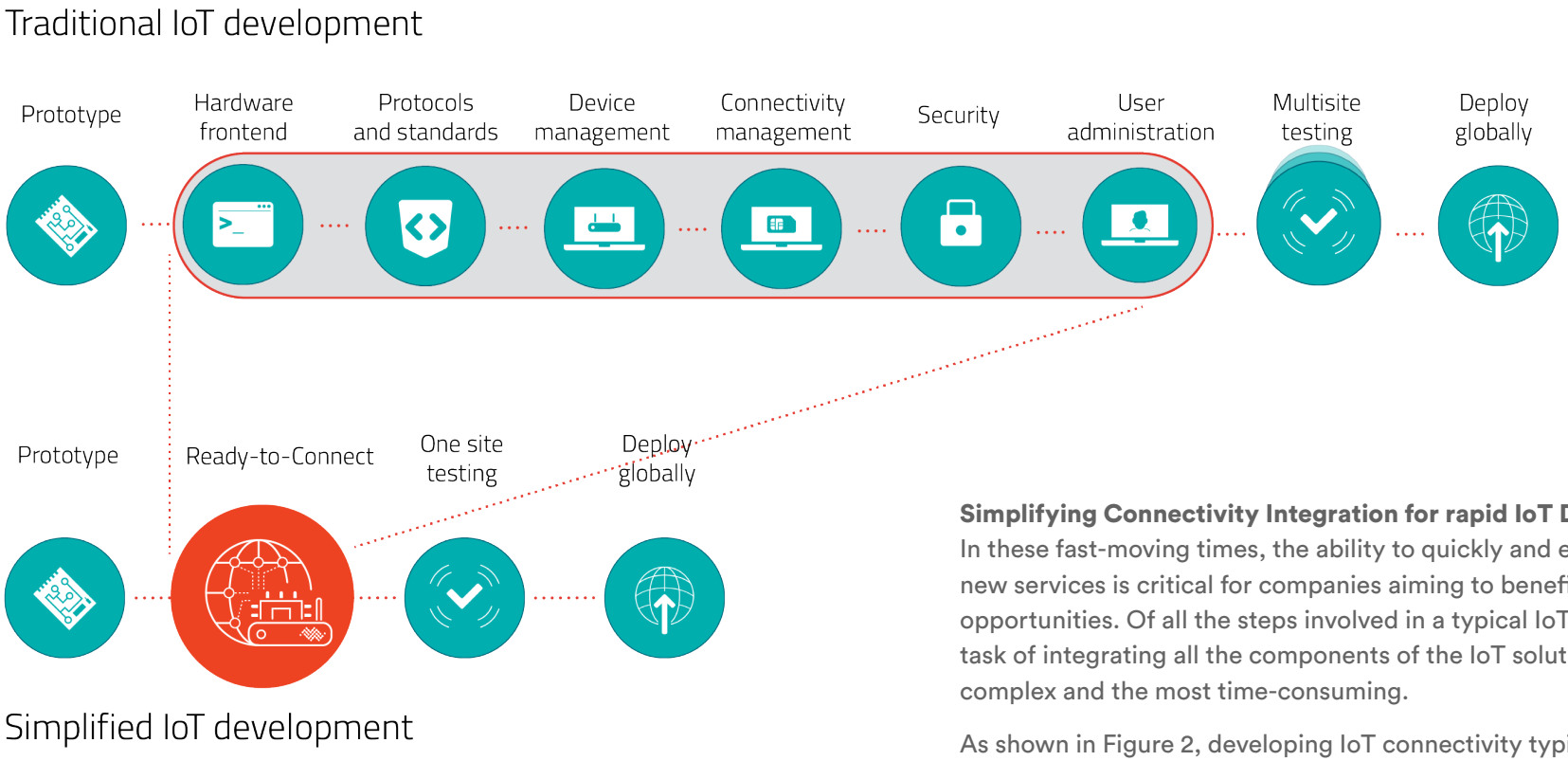
One Point of Accountability and Management

The One point of Accountability feature provided lowers the time it takes to identify the root cause of any anomalies or outages in the connected device. High levels of security are needed in order to ensure there is no interference with data transfer and the Sierra Wireless solution provides an intrinsic end to end view of security across the entire production chain. Ready-to Connect uses a layered approach with different security mechanisms built into every component of the solution (device, network, cloud), along with end-to-end schemes, thereby ensuring the appropriate level of security. It also provides a single point of responsibility for the overall security solution. These various security measures work together to protect the deployment, minimise the risk of any loss or theft, and significantly reduce the financial risk of running an IoT-enabled service.

WEBSITE

SIERRA WIRELESS®

Figure 2. *Simplifying connectivity integration with Sierra Wireless Ready-to-Connect*



Simplifying Connectivity Integration for rapid IoT Deployment

In these fast-moving times, the ability to quickly and efficiently launch new services is critical for companies aiming to benefit from emerging opportunities. Of all the steps involved in a typical IoT deployment, the task of integrating all the components of the IoT solution is often the most complex and the most time-consuming.

As shown in Figure 2, developing IoT connectivity typically begins with prototyping, moves through the many steps of integrating products and platforms, and is then followed by multi-site testing and global deployment. The multi-faceted integration phase is where all the IoT elements come together. It can be a challenging exercise since any issues of interoperability can be costly to address and time-consuming to fix after solution roll-out.

WEBSITE

Sierra Wireless' Ready-to-Connect Solution lets IoT teams skip many of the complicated, time-consuming steps commonly associated with the integration phase. The solution includes pre-connected modules and routers, equipped with an integrated global eSIM, and works with the Sierra Wireless IoT Platform to securely manage devices, connectivity and application data.

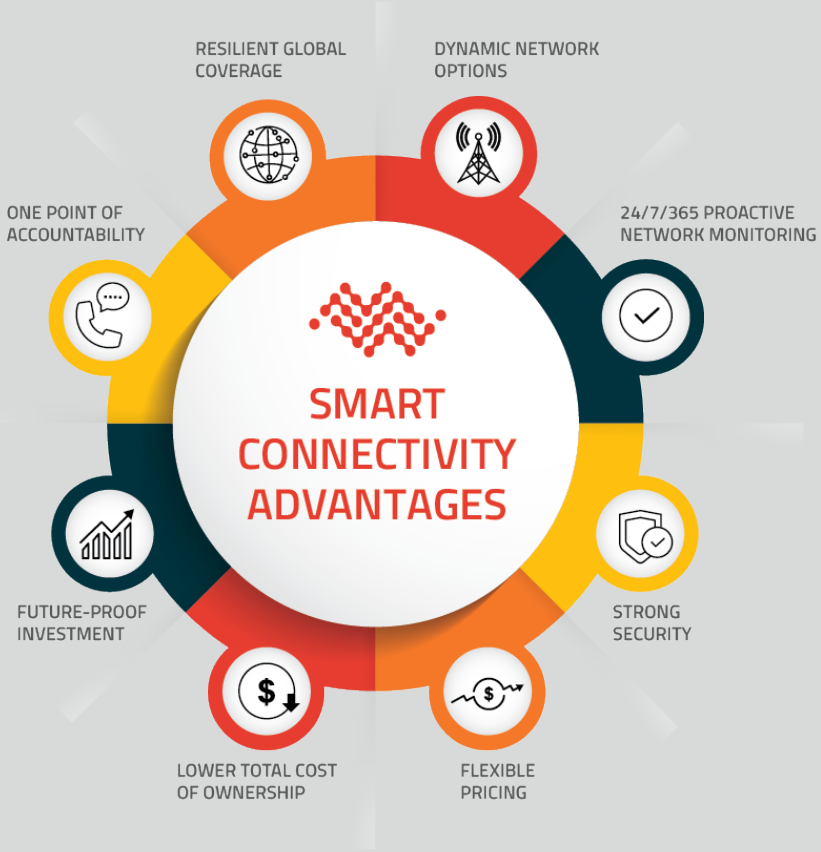
Key management challenges

Businesses are becoming more reliant on their IoT connectivity as services evolve, with greater emphasis on overall cost reductions as well as increasing revenue expectations. It is one thing to select the most appropriate IoT connectivity to fulfil the needs an IoT project, quite another to manage it in the field. This is especially the case where the applications to be connected are already business-critical or likely to become so.

Faced with these significant challenges, Sierra Wireless offers its Smart IoT Connectivity suite, offering major advantages as shown in Figure 3.

Sierra Wireless simplifies connectivity choices by delivering the device, software and service solutions needed to accelerate IoT deployment. Innovative products, solutions and services connect thousands of businesses to critical data and millions of people to information. The company remains focused on developing leading technology solutions and on empowering businesses and industries to transform and thrive in the connected economy so they can reduce complexity and turn data into intelligence in increasingly business-critical situations.

Figure 3. *The Advantages of Sierra Wireless' Smart Connectivity offering*



WEBSITE

software AG

Critical processes require an industrial edge

High-value assets. Heterogenous devices. Harsh environments, often with limited connectivity. Complexity and high stakes make industrial edge computing uniquely challenging.

Edge compute capabilities are becoming essential where low-latency control of machines is critical; where communications might be unreliable, and downtime is not an option; or where the amount of data generated or the network bandwidth available makes it undesirable to transmit everything to the cloud.

Industrial edge uses for smart manufacturing include requiring precise adjustments to be carried out every millisecond; collecting large amounts of data that need to be aggregated before sending to the cloud; or for wind farms where the turbines need to be systematically feathered in high winds, but where the weather conditions could coincide with network downtime.

> ***We have a very open partnership with Software AG. We have infinite knowledge in the area of machinery and data detection and they have exceptional knowledge of data capture and analytics through IoT. Ours is the perfect union.***
>
> Oliver Prang, Expert Digital Business Development, SMC Deutschland

How edge overcomes typical challenges in industrial IoT

REAL-TIME PERFORMANCE

Challenge: Real-time actions based on machine data is essential to avoid machine downtime, higher repair costs, or poor product quality, and the roundtrip to the cloud can take longer than the time window for a successful outcome.

Solution: Cumulocity IoT Edge can deliver low network latency and fast response times, a critical advantage when dealing with high value assets where the cost of every minute of downtime rapidly decays value.

UNRELIABLE CONNECTIVITY

Challenge: Predictable continuous monitoring is required to ensure that the actions to remotely manage critical industrial equipment is based on a reliable stream of measurements, regardless of the bandwidth or performance of the connection.

Solution: Cumulocity IoT Edge ensures a sequential stream of measurements are received by the remote hub regardless of connectivity bandwidth constraints or intermittent dropouts.

SECURITY & CONFIDENTIALITY

Challenge: Equipment used to manage critical infrastructure (like electricity grids), medical facilities (like laboratories) and government facilities (like emergency services) cannot be reliant on cloud infrastructure or public networks alone.

Solution: Being completely self-contained, communication network agnostic and deployable stand-alone, Cumulocity IoT Edge offers machine makers comprehensive computing capabilities which can be embedded in secure environments.

WEBSITE

software AG

COSTLY CONNECTIVITY

Challenge: Some geographic locations have extremely limited connectivity options, which can make the cost of remotely monitoring deployed machines prohibitive, especially if the transferred data volumes are high.

Solution: Cumulocity IoT Edge can significantly reduce the transferred data through pre-processing the data prior to transmission, sending the processed metrics, and only sending the raw data when essential.

LOCAL AUTONOMY

Challenge: Highly reliable processes require the control of local machines to be based on local measurements and the operation of local actuators with no dependency on the availability of external compute resources.

Solution: Cumulocity IoT Edge is a complete fully autonomous package that allows on-site execution of sophisticated condition monitoring or predictive analytics that can be created by field engineers without data science training.

SPOTTING ANOMALIES

Challenge: Trends that indicate the potential for a future problem are often hidden by the massive number of high-frequency measurements generated by modern industrial equipment that is uneconomic to transfer for data analysis offline.

Solution: Cumulocity IoT Edge allows machine learning models to be created and deployed to continuously analyze the data for previously identified failure fingerprints, assess trends, and capture operational outliers.

Avoid common pitfalls and scale at the edge

The challenge with IoT can be that, while an organization's operational teams (OT) and IT teams are typically aligned on areas such as security, differences between the core needs of each in other areas contributes to up to 75% of IoT projects failing.

Operational teams require robust technologies that enable them to be self-sufficient to innovate, while IT need systems that support their existing infrastructure to integrate IoT with their existing business systems.

Cumulocity IoT takes an approach that supports the needs of both. Operational experts can use their domain knowledge and leverage the self-service capabilities of the platform to create innovative solutions that increase operational efficiencies without the need to write code. Crucially, for complex use-cases, IT can still customize and extend the platform. Due to its open architecture, it's possible to integrate Cumulocity IoT in a secure way with existing enterprise applications and infrastructure as well as seamlessly port between edge, cloud and on-premises.

Cumulocity IoT's flexibility makes it straightforward for machine makers to start their IoT journey with an edge-based IoT solution and then seamlessly extend this to the cloud, through the unified experience across various deployment options (on-premises, cloud, and edge).

The edge capabilities deliver the capabilities of the full IoT platform, including advanced analytics to efficiently analyze real-time data all with a footprint suited for low-powered edge devices.

Analytics, protocol adaptors and IoT apps can be shared across all environments (in the cloud, at the edge, on-premises) and, with support for resource constrained edge devices and industrial protocols, Cumulocity IoT makes it possible for equipment makers to push the boundaries of what's possible.

WEBSITE

software AG

Start any way that works for you

Meet our IoT edge platform
www.softwareag.com/iot-edge-computing
Discover Cumulocity IoT Edge

Free trial www.softwareag.com/iot-free-trial
Try Cumulocity IoT for 30 days free.

Developer community www.softwareag.com/iot-developer
Join the discussion. See what others are saying – and building.

WANT TO ACCELERATE YOUR IOT INITIATIVE?
Cumulocity IoT Quickstart is a fixed-fee, consulting-led, cloud delivered engagement that accelerates the delivery of your 90-day pilot in four phases:

- Start & scope – including a discovery workshop to explore your IoT goals
- Architecture & design – with a deep-dive workshop looking at "as-is" and "to-be" architectures
- Development & test – with continuous support from software AG consultants
- Review & extend – including measuring outcomes against success criteria

> ***We have put extremely powerful analytical tools into the hands of those that understand the production process the best opening a new era of streamlining and improvement.***
>
> Manager Digital Factory, Dürr

About Software AG

Software AG is the software pioneer of a truly connected world. Since 1969, it has helped 10,000+ organizations use software to connect people, departments, systems and devices. Software AG empowers truly connected enterprises using integration & APIs, IoT & analytics and business & IT transformation. Software AG's products establish a fluid flow of data that allows everything and everyone to work together. The company has more than 4,700 employees across more than 70 countries and annual revenue of over €800m, with the aim of exceeding €1bn by 2023.

WEBSITE

SONY

How to Succeed in Building Cellular IoT Devices

In the heart of any IoT ecosystem, there are devices which act as the backbone, aggregating and communicating the data to the cloud. Our long-time presence in the IoT market has given us deep insights into the unique requirements of these devices, being very low on resources while demanding adequate performance and reliability. Using these insights, we've specifically designed our Altair ALT125x cellular IoT chipset solutions to address the challenges. Let's review the top challenges for designing a cellular IoT solution:

1. Low Power

IoT devices need to operate on very low power, enabling long battery life to ensure the solution is functional for many years, sometimes over a decade. The ALT125x was designed from the ground up to consume ultra-low power, enabling connected applications with battery life of over 10 years. This is achieved by leveraging Extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM) features of GSMA's LTE-M and NB-IoT cellular IoT protocols on the protocol level, combined with dedicated power management design on the chip level, minimizing chipset power consumption in various sleep and operating modes of the device.

Sony's Altair cellular IoT chipsets are known for being ultra-low power, achieved through state-of–the-art VLSI techniques, sophisticated algorithms and high-efficiency architecture and system design. Sony's Altair proprietary SoC with dedicated power optimization technics and software implementation, maximizes battery life of cellular chipset designs.

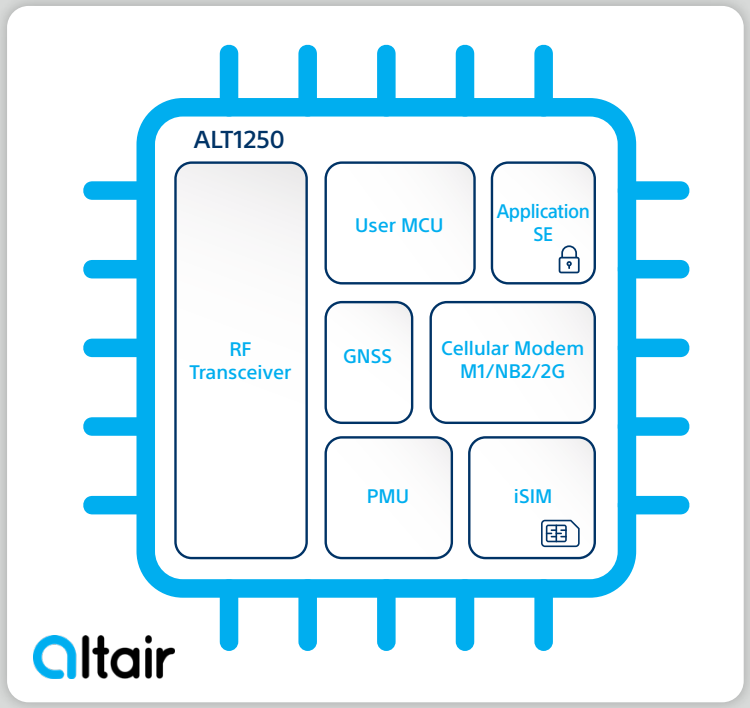
2. Compact Size

IoT devices also need to be portable and compact, to allow flexible and secure placement of the device per application needs, as well as easy installation. Many IoT applications – from wearables to sensors and trackers – require small modules with minimal X, Y and Z dimensions. Sony's Altair highly-integrated cellular IoT chipsets – the smallest in the world (enabling LTE-M and NB-IoT modules as small as 10×10 mm2) – minimize external component count and are available in a variety of packaging options to fit the size constraints of various applications.

3. Integrated Components

Featuring highly integrated design, Sony's Altair ALT125x comes packed with powerful Cortex-M MCU for application development, used as the platform to execute higher level protocols required to communicate with the cloud such as MQTT or the COAP based LWM2M - the most (standard-based) efficient protocol. See figure 1.

Figure 1. *Sony's Altair ALT125x integrates all required components for cellular IoT applications*



WEBSITE

SONY

Determining and tracking IoT device location is essential for many markets and applications. Integrated GPS capabilities enable Sony's Altair chipsets to provide cohesive location services for enhanced positioning capabilities without increasing the size and cost of the module. Sony's Altair integrated GPS technology, inherited from parent company Sony Semiconductor Solutions Corporation, also offers unparalleled integrated battery performance.

4. Seamless Connectivity

Operating in these restrictive conditions, devices are required to provide seamless and ubiquitous connectivity in any geographic region and support mobility between regions for applicable use cases. A cellular IoT device must autonomously decide when to search for a network and which to connect to – based on low data-connectivity costs, and 'good enough' coverage. In addition, the need to support more than one RAT (radio access technology) doesn't make it easier. The diverse global spectrum band allocation or the different RAT options should not be an obstacle for module and device vendors. To ensure multi-market and versatile carrier support, Sony's Altair breakthrough OneSKU™ RF technology enables support of any LTE band combination on a single hardware or module design. Sony's Altair ALT1250 features dual mode NB-IoT and LTE-M RAT options packed in a single design, providing module and device vendors with a truly global solution without increasing solution size or cost.

5. Security

Security in the IoT era is crucial and Sony's Altair chipsets integrate a multi-layered security architecture to address these requirements. Featuring chip and device hacking-protection as well as a robust service access layer, Sony's Altair chipsets provide the most advanced hardware- and software-based tools to ensure end-to-end security.

Sony's Altair ALT125x family delivers the highest security standard, with the world's first commercial integrated SIM offering. The SIM module is integrated into the chipset and has been approved by multiple Tier-1 MNOs, as well as the leading SIM OS vendors. This level of security has been extended to serve the application needs, by allocating a dedicated security element with its own memory and peripheral interfaces.

Complementing the strong technical offering of the ALT125x family, Sony Semiconductor Israel had also built a strong network of partnerships over the last years, resulting in ALT125x devices selected as the connectivity of choice in all tier-1 module vendor solutions, and certified with all tier-1 network operators worldwide. This level of market adoption ensures customers have a proven, certified all-in-one Cellular IoT solution.

altair

WEBSITE

SONY

A Technologist's View of the Integrated SIM (iSIM), Featuring Rotem Gazit, CEO of Arad Water Meters

What are the challenges you are solving for your customers?
Our clients mainly include water utilities around the globe that provide water to residential areas and are looking for high reliability and accurate measurement solutions. We help our customers lower the "waste of water" which is the difference between the amount of water provided by the utility and the amount that is billable to the end customer.
In addition, Arad's advanced smart metering infrastructure provides 24/7 monitoring for leaks and breaches, combined with advanced features like integrated pressure sensors.
In general, our R&D and operational challenge is to build affordable measuring devices that guarantee 10 to 15 years of real time constant unmanned service.
Arad also plays a part in society. For example, in the face of the recent COVID-19 pandemic, Arad, in collaboration with the Israeli social services, initiated the "Living Water" program to use Arad's advanced solutions to protect elderly, solitary people who don't have frequent visitors to their homes due to social distancing. We monitor the water consumption of these lonely individuals. If we detect a day without water consumption, Social Services are automatically alerted through the system. They then send a representative to check on the person's condition before it is too late.
To recap: We offer the products and infrastructure to support a vital service – providing water to people's homes. Our customers expect 100% reliability from a product that is exposed to harsh environmental conditions and has to keep measuring accurately for 10 to 15 years in a cost-effective way to support large-scale deployment.

Where do you see the promise of iSIM and its potential for the Aead Group?
Fundamentally, we are looking for data integrity. It is crucial that the communication device in the field and the data measurements sent to the network can be trusted. iSIM enables all of this, with additional benefits including saving Bill of Material costs by eliminating additional hardware components and increasing product reliability by eliminating the external SIM card or chip.
iSIM also reduces power consumption which is critical. As our product works with irreplaceable batteries, we need the power consumption to be as low as possible in order to increase the meter's lifetime. The iSIM that is tightly integrated in the modem chipset already implements all the required low power modes and consumes less power than a standalone solution.
From a logistics perspective, iSIM provides an opportunity to provision devices before being deployed – using one hardware SKU while supporting different carriers and countries.

Much like you, others might be wondering how they can choose between many confusing options. What questions should technologists be asking, to know that iSIM is the right choice for them?
The fundamental question for a technologist is whether their selected partners can offer a secure and approved SIM for their targeted carriers. Standardization efforts are in the right direction. As standards are currently being established, this will accelerate the rate of technology adoption by carriers and encourage additional chipset makers to bring this technology to market.

https://www.youtube.com/watch?v=xWRw7-mOjQk

WEBSITE

WNDRVR

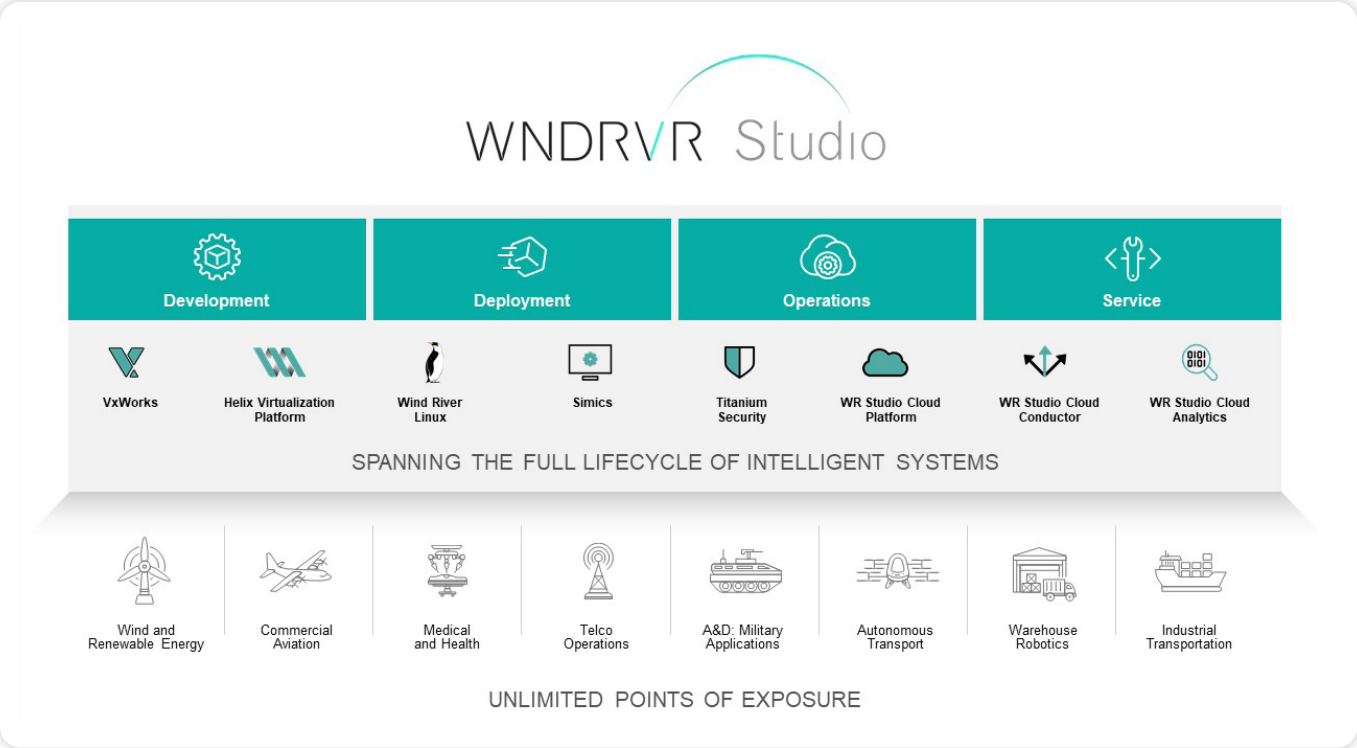
The Intelligent Systems Future

In our increasingly digital world, intelligent systems represent the next wave of the digital machine economy. They encapsulate the synergistic combination of intelligent IoT devices and intelligent edge computing with more recent developments, notably 5G, AI and cloud-native technologies. Leveraging those developments to deliver the full potential of an intelligent systems environment is enabled by Wind River Studio, the first cloud-native platform for mission-critical intelligent systems.
Features include:

- Having full system visibility through single pane of glass architecture
- Mission-critical capability, agility and workload durability for the Intelligent Edge
- Leveraging cloud scale with infinite compute power and deployment through to a mission-critical far edge cloud
- Maximising efficiency through the automation of workflows across functions
- Unified orchestration and analytics across public cloud, far edge cloud and physical devices
- End-to-end security through a single sign-on system for tools and workflows, identity management and access controls
- A platform that powers 5G virtualized infrastructures.

The Studio offering has the proven ability to allow developers to develop, deploy, operate and service on the edge in near real time; to build secure, safe and mission critical capabilities; and to operate in near real time on the far edge.

Figure 1. *Wind River Studio – Spanning the Full Lifecycle of Intelligent Systems*



WEBSITE

WNDRVR

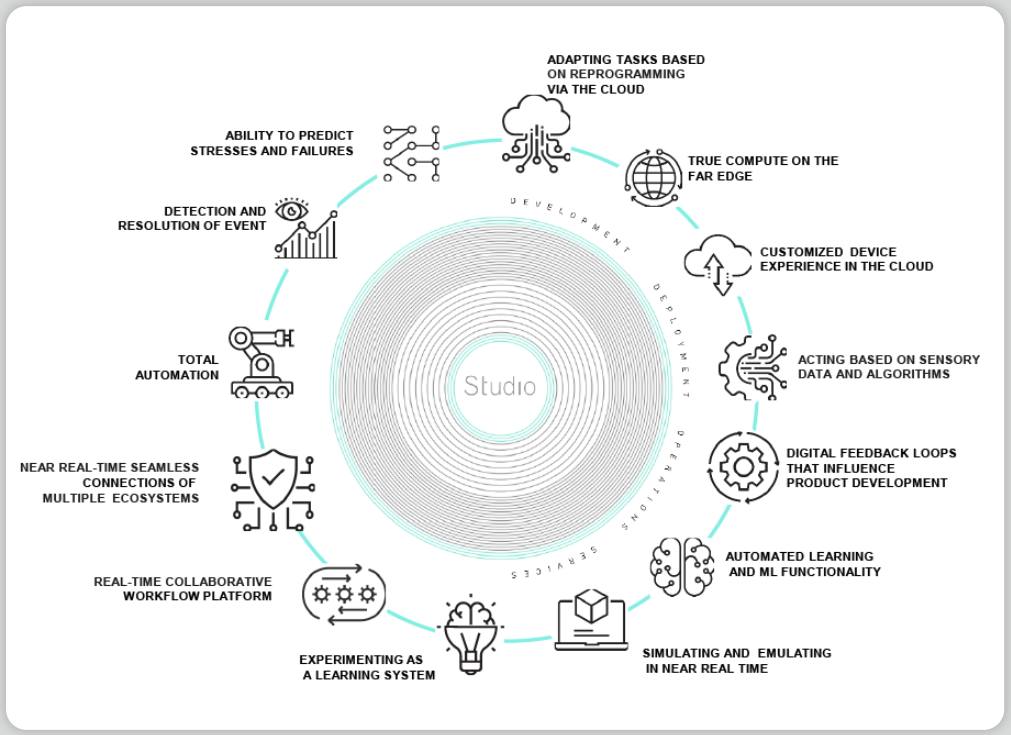
Develop
Studio reengineers development workflows into solution sets that reduce development costs and accelerate capabilities for building, testing, and deploying on the edge. Highlights within the develop phase of Studio include the ability to develop for virtualized infrastructure or optimize for hardware, easily adapt solution for new features or hardware, and automate re-validation to enable continuous deployment.

Deploy
Studio provides the widest choice of deployment options, spanning safety-critical systems, edge devices, distributed edge cloud or public cloud. Highlights within the deploy phase of Studio include flexible deployment scenarios through a common platform, ability to easily span device and edge infrastructure, and access to market-leading OS portfolio and open-source solutions.

Operate
Studio delivers an integrated cloud platform unifying infrastructure, orchestration, and analytics capabilities so operators can deploy and manage their intelligent 5G edge networks globally. Highlights within the operate phase of Studio include a single end-to-end platform for orchestration and operation, proactive optimal network operations, as well as deeper, broader, and tailored data.

Service
Studio offers a range of services, including managed services, security, safety and certification, lifecycle management, education, and customer support.

Figure 2. *The 13 characteristics of intelligent systems.*



WEBSITE

WNDRVR

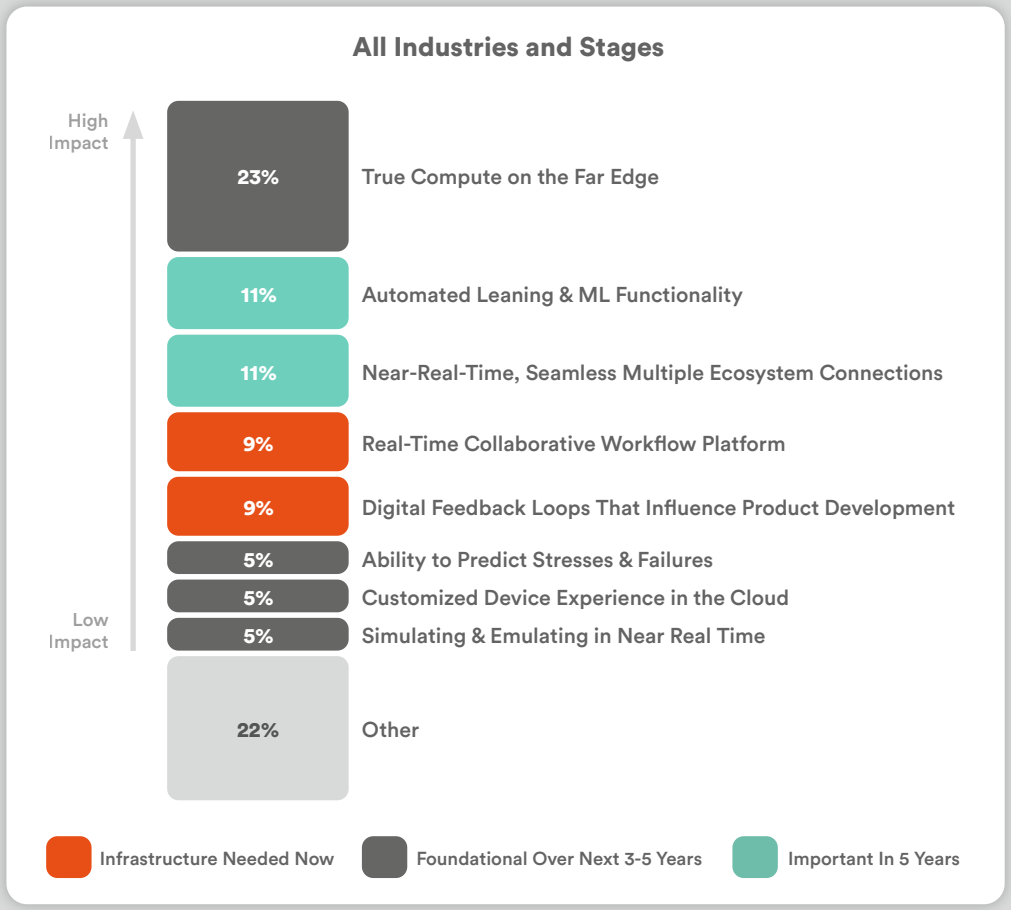
According to Wind River research, intelligent systems success depends on properly timing the implementation of the 13 key intelligent system characteristics shown in figure 2. These deliver different levels of positive impact depending on sector and stage of intelligent systems development, and ultimately support a rapidly evolving intelligent systems machine economy. These characteristics map to the multi-faceted view of Studio capabilities across the four phases of the intelligent systems lifecycle.

The stacks in figure 3 represent the magnitude of business impact each intelligent system characteristic has on an intelligent system. The larger the block, the greater the impact. Individual sector ratings cover Manufacturing, Aerospace/ Defence, Automotive, Energy/Utilities, Medical and Telecommunications.

For more details about Wind River intelligent systems research, see: https://www.windriver.com/intelligent-systems

For more details about Wind River Studio, see: https://www.windriver.com/studio

Figure 3. *Business impact ratings of key characteristics – average across all industries and stages of deployment.*



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

facebook.com/BeechamResearch

linkedin.com/company/beecham-research

beecham research

Shaping the IoT future