Why IoT Projects Fail

And What To Do About Them

Four Key Elements for Sustained IoT Success

Sponsored by:

pod group

beecham research

Shaping the IoT future

IoT adopters have grave concerns about the security of their devices and networks according to research carried out by IMC (the International IoT M2M Council). The study, commissioned by Pod Group, questioned over 20,000 IoT adopters including IT, operations and product development managers and board-level decision makers. Security was the biggest challenge to IoT deployments. The adopters were extremely concerned about threats to their devices, however only a quarter of respondents are currently using additional dedicated IoT solutions, while a further quarter were actively looking for solutions.

The study also found that adopters would like to have access to in-depth security information and around half would like to see detailed analytics and custom reports.

IoT is clearly at a critical tipping point. On one hand advances in technology mean that it's cheaper and easier than ever to produce "smart" devices, equipment and machinery that deliver significant benefits: benefits that the business community cannot afford to ignore. On the other there are equally significant challenges such as the skills shortage and complexity of large IoT projects, so these may and often do result in expensive failures. For example, in May 2017 Cisco was indicating a failure rate of 75% and in July 2019 Microsoft stated that 30% of IoT projects failed in the proof-of-concept stage.

There are numerous reasons why IoT projects fail. For example, a disconnect between technology and business outcomes. IT decision-makers may place more importance on technologies, organizational culture and expertise while business decision-makers place greatest emphasis on strategy, business cases, processes, and milestones. Invariably, business aims and system architecture are not thought out. Companies may fail to appreciate IoT's broader implications and complexity compared to regular IT projects.

There is little to be gained by identifying other systemic reasons. Viable, cost-effective solutions are being realized by many companies operating in the leading industrial vertical sectors: manufacturing, transportation, oil and gas, mining and healthcare. Instead we are going to highlight three intrinsic issues that companies typically encounter when deploying a solution that has passed the proof-of-concept stage. The first comes when the IoT solution is connected to the network that has been selected. The second from management of the deployment. The third is the security of the network.

There is a fourth issue, one that reflects the relatively recent creation of solutions that enable companies to transition from revenues based on one-off purchases to one that generates on-going revenue streams, e.g. subscription-based services.

1. Connectivity

Companies may not be aware of the business and technical networking issues. For example, incompatibility of the network with the various connectivity options of the modems employed by the devices. Hardware choices should be made after the connectivity decision, not before, otherwise the required service may not be feasible.

2. Management

If the solution is rolled out in different countries on different networks it is difficult to manage the data centrally. Troubleshooting is complicated if there is limited visibility into the SIM's behavior and data volumes increase the complexity of trying to troubleshoot and manage individual IoT devices.

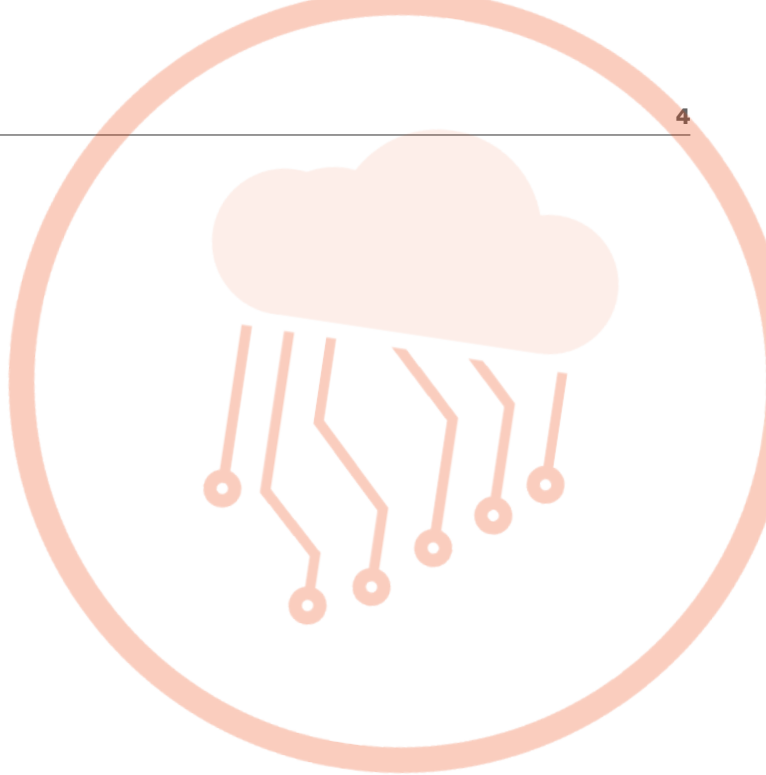
3. Security

The security of IoT solutions is the number one concern for the business community and there are valid issues concerning network and device security. Pod Group's own research confirmed this concern. Fraudulent use of SIM cards is one issue, but there are many other security issues specific to IoT deployments. IoT devices are difficult to secure, computing resources are limited due to their small form factor, and software patching is problematic. And the attack surface of IoT's value chain is an attractive target for hackers.

Security solutions must also comply with recent legislation, e.g. in California, beginning on January 1, 2020, devices must have a reasonable security feature or features. And in the U.K., there is a Design Code of Practice that advocates for stronger cyber security measures to be built into smart products from the design stage.

4. Billing

Billing issues may also arise after a successful deployment since they become more complex as the project scales. Companies that are focused on product sales may not have the tools needed to monetize subscription-based services. And systems integrators who are managing a complex supply chain of resellers and distributors need a robust way of managing and billing their customers.



Addressing connectivity issues

Pod Group is a leading MVNO with more than 20 years of experience in M2M and IoT connectivity and over that time the company has worked closely with customers who have encountered the kind of problems outlined earlier and incorporated the requisite functionality into the Pod product offering. This has been a continuous process, one that has accelerated in recent years, in line with IoT developments and deployments. Moreover, the company has not only tracked them, but it has also anticipated them and updated the offer, which includes consultancy and testing services.

Updates include the integration of IoT specific connectivity, e.g. Cat-M and NB-IoT, as well as a comprehensive range of SIMs: including native single network, data roaming multi-network, multi-IMSI and eUICC. This technology agnostic offer currently operates on 600+ networks in 185 countries. The company's Connect module, which is part of Pod IoT Suite, Pod's modular IoT connectivity platform, provides all these connectivity options. Moreover, the Pod Manage module enables them to be managed from one interface. Other connectivity options can be integrated via an API.

The need for back-up and redundancy for mission critical and remote applications would seem to be obvious, but some companies only find out when they experience a problem. When devices are constantly crossing borders, multi-IMSI SIMs provide redundancy and resilience, OTA enables remote management of SIMs in the field, and eUICC provides the flexibility needed for remote applications that are difficult to access. In addition, a multi-IMSI SIM app avoids points of failure on the network by automatically swapping to a completely different network infrastructure in case of an issue on the core network.

IoT devices have limited resources but Pod SIM Cards, unlike regular SIMs, can augment the communications and computing resources and enable "regular" devices to perform additional tasks. Light SIM applets can be downloaded and updated over-the-air in order to address connection issues, facilitate deployment and enhance device security.

Key benefits:

- Network agnostic offer means any global network can be integrated, managed and billed via one platform, including a company's existing IMSIs
- Native network agreements (e.g. all US networks) provide the best local rates in-country
- Global multi-network offering covers 600+ networks in 185 countries
- Multi-profile eUICC specification on any form factor, enables native and global services to be combined on one SIM to achieve the best rates
- eUICC with Pod Profile incorporates intelligent SIM apps to control QoS, security and roaming functionality
- Onboarding service including device compatibility testing and consultancy
- 24/7 expert technical support
- Real time tracking of any SIM stolen from a critical device
- Modification of the devices allowed to use the SIM (white list)
- Remote control and network updates to the SIM including preferred network and network blocking (FPLMN)

Figure 1. *Pod IoT Suite is a modular platform that connects, manages, secures and bills IoT applications. The modules can be employed on their own or in conjunction as parts of an integrated connectivity solution.*

Addressing management issues

As indicated earlier, if the solution is rolled out in different countries on different networks, centralizing the management can be problematic especially when dealing with multiple carriers on multiple APNs. Centralized troubleshooting, connectivity analytics, network diagnostics and support are needed for this task as well as providing customers with the functionality to scale the deployment. And troubleshooting is complicated if there is limited visibility into the SIM's behavior.

The Pod Manage module of Pod IoT Suite enables all the connectivity options on a customer's account to be managed, billed and secured centrally via one platform, regardless of whether they include different global networks, or even different connectivity technologies. This enables real-time control of the SIMs plus the ability to quickly identify and resolve connectivity issues and perform advanced analytics and diagnostics. This is a standard feature with all Pod Group IoT SIM cards. Functionality includes activation of the SIMs, setting data limits, performing SIM diagnostics and receiving precise troubleshooting advice.

Key benefits:

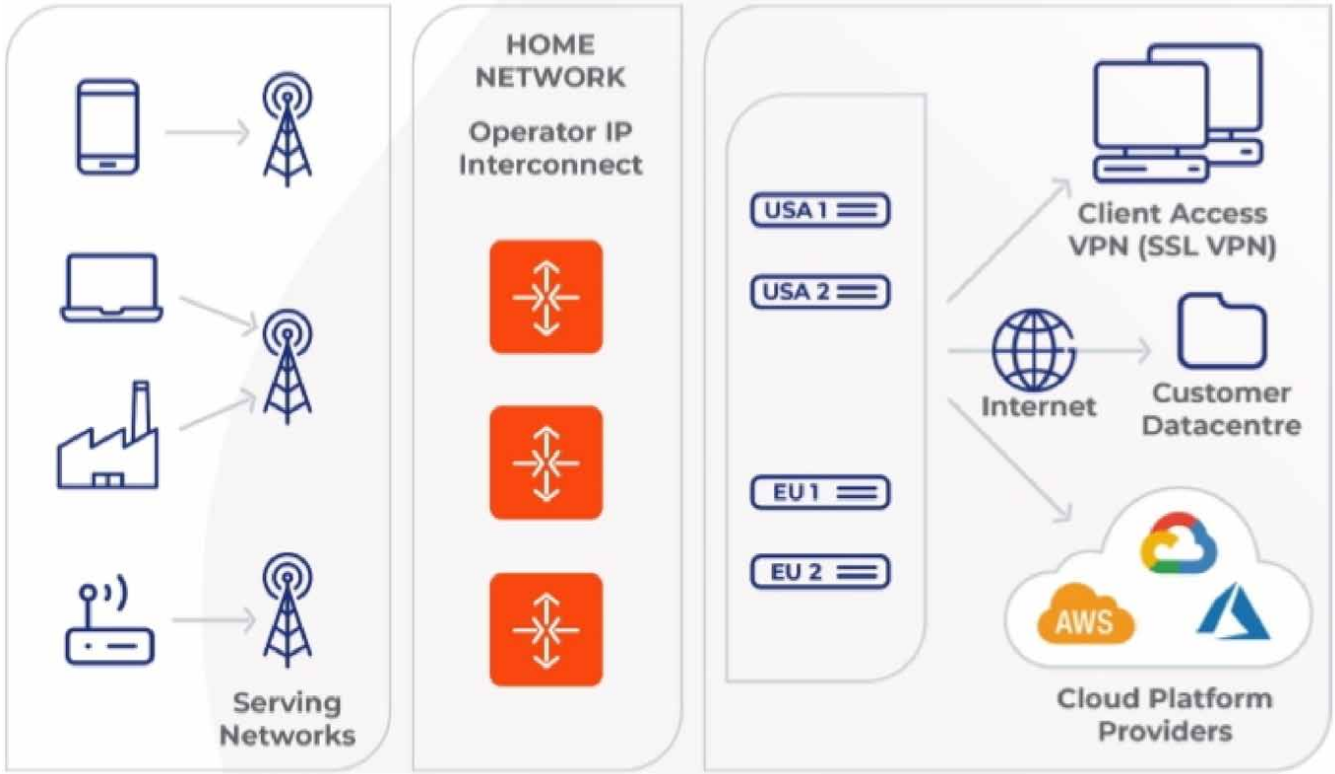
- Easy integration of additional connectivity options/networks. API available for integration with other platforms e.g. device management
- Management platform standard with all Pod IoT SIMs. White label instance available with customized branding.
- Multiple hierarchies enable management of complex channels of distributors and resellers, or subsidiaries in different locations.
- Advanced SIM diagnostics and troubleshooting plus 24/7 support service
- Instant diagnosis of SIM issues
- Management of SIMs on the move. Pod Suite for Android and iOS devices enables mobile management

Addressing security issues

This is the single biggest IoT issue, the top-of-mind concern for the business community and Pod Group has made it the cornerstone of the company's comprehensive connectivity offer. The company operates its own distributed IP core network through four points of presence (PoPs), two in the USA and two in Europe. Each site has Gigabit Ethernet connectivity with the third-party serving networks of MNOs as well as Pod data centers.

This network architecture is used for all Pod traffic as well as the delivery of IoT data to the company's customers and Cloud platform providers. It is a state-of-the-art MVNO infrastructure that segregates IoT traffic from the public Internet, thereby blocking off the regular source of security attacks.

Figure 2. *Access to Cloud providers is facilitated by an on-demand private connectivity service that allows bandwidth and duration to be set up on the fly. The Connect service uses private, dedicated connections that function as if they were part of a customer's own network. Alternatively an Internet connection can used to provide an Internet VPN service.*

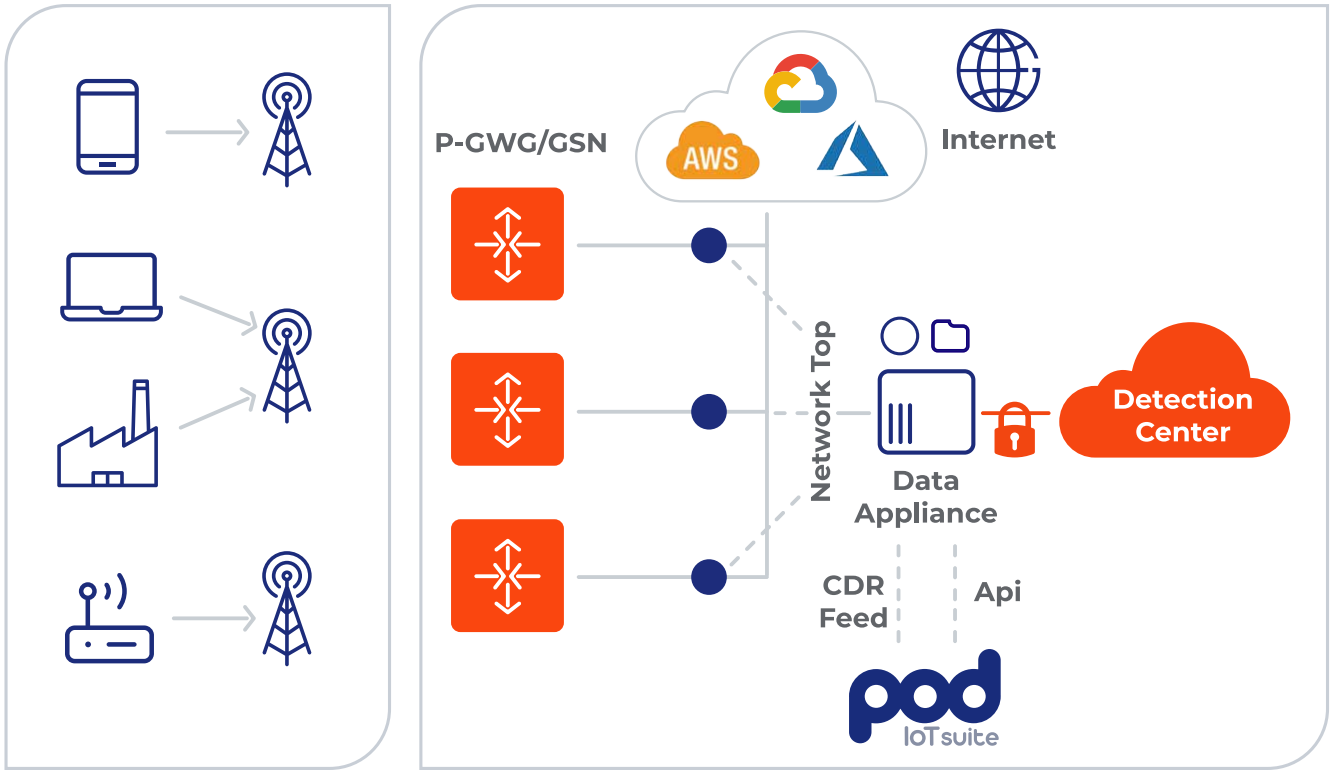


Pod Connect

Pod Connect is an enhanced connectivity solution that has private IP address space for network address allocations and at each PoP traffic is routed onwards according to IP Policy and routing rules. Connectivity links go directly from this network into the customer's data center or a cloud service. The result is a private stable and secure data channel.

Regular Internet VPNs offer an extra layer of security through encryption, but data is still routed over the public Internet so is still exposed to security threats and disruption due to DDoS and other network outages. The Pod Connect VPN service is delivered using private, dedicated connections, as if they were part of a customer's own network. It is a site-to-site service that operates from the network POPs.

Figure 3. *Pod Connect monitors traffic coming from the POPs and runs it through a Data Appliance in order to determine the type and the source. Anomalies are flagged in the Detection Centre and a feed is sent to the Pod IoT Suite where it is presented to the user.*



Pod Protect

Pod Protect is an agentless, network-based security monitoring product that can monitor billions of devices and their data transmissions. It employs a three-tier detection strategy: signature-based, heuristics and anomaly-based as well as machine learning to detect anomalies on the network. Alerts are generated if anything suspicious occurs and it learns which traffic is normal for each device. The threat database is updated in real-time with signatures from 48 sources located in key cities around the world.

Key benefits:

- Distributed IP core network; data does not touch the public Internet
- Direct connectivity at each peering location, or via Pod's connectivity partners
- Private IP address space for network address allocations
- Internet VPNs employ IPsec or IPsec encrypted GRE Tunnels
- Traffic routed and treated differently according to the customer and sub-network
- Agentless security monitoring; no changes need to be made to the device
- Machine learning algorithm compares its findings with real-time global threat updates to improve detection

Addressing billing issues

Pod Group buys wholesale airtime from leading MNOs, including native agreements with all North American operators. Globally, roaming agreements provide access to 600 networks in 185 countries. The airtime is retailed along with a comprehensive service portfolio. Operations are conducted in an ultra-competitive market, which means that the billing process is very complex. Charges are conducted in local currencies and different data plans. But the only thing that counts is the ability to produce accurate, detailed bills, otherwise customers will switch and be lost.

Connectivity retailers face a similar challenge, but so do the vendors of IoT products and services. Complex supply chains of suppliers and distributors have to be managed and billed, as do the vendor's customers. Moreover, in many sectors outright product sales are being replaced by subscription services. Therefore the billing process must enable recurring revenues to be captured and managed.

These requirements were anticipated when the Pod Bill module was created; originally developed for the complex subscription-based billing scenarios that arise when customers require centralized billing from a variety of different service providers, it was designed to be agnostic. Subsequently the functionality was abstracted from connectivity in order to enable anything that can be quantified to be billed. Abstraction allowed the company's billing services to be extended to non-cellular connectivity services such as SigFox and LoRa, and also opened up the possibility to customize billing for other products, such as hardware and software. The availability of a white-label instance of the Pod Bill module means that resellers can bill their own hierarchy of distributors and end users under their own brand.

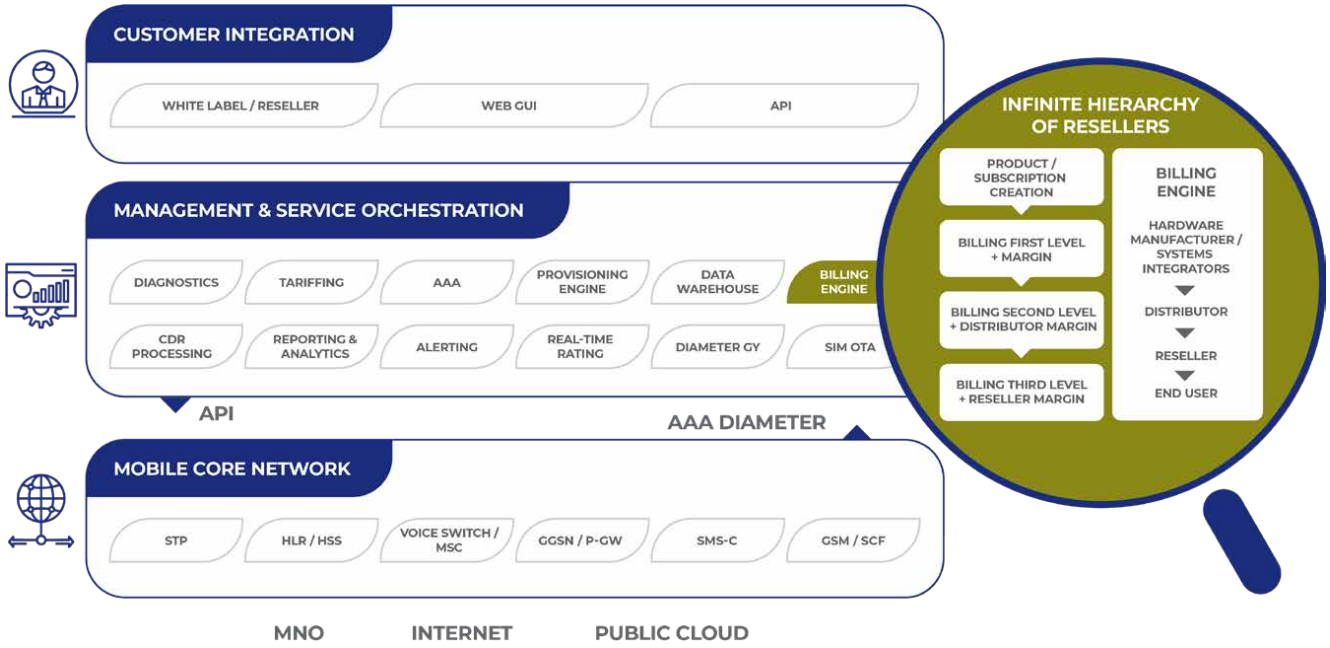
As shown in the following schematic, Pod Bill provides near real-time visibility of services as they are being used, thereby enabling granular control of the billing process. Having detailed, up-to-date information prevents bill-shock and facilitates the management of large SIM deployments. It also enables control of SIM usage data by providing detailed, graphical analytics, for example, subscriber usage over the past 24 hours, week or 30 days. In addition it enables integration of mobile services from multiple MNOs within a single billing and operational support system.

The product creation engine enables control of the billing cycle, contract length, billing dimensions, and currency as well as how customers are billed: per usage, data bundle subscriptions, and data pooling.

Key benefits:

- Turn-key, integrated white label billing
- Full hierarchical resale and re-rating capability
- Flexible middleware micro-service integration
- Control the billing cycle, contract length, billing dimensions and currency
- Near real-time visibility of services as they are being consumed
- Manage large SIM deployments and avoid bill-shock
- In-depth graphical analysis of subscriber usage over the past 24 hours, week or 30 days
- Manage subscription usage and identify trends
- Automatic generation of session usage and billing reports

Figure 4. *The product creation engine enables control of the billing cycle, contract length, billing dimensions, and currency as well as how customers are billed: per usage, data bundle subscriptions, and data pooling.*



SIMs and SIM technology

Pod Group markets a comprehensive range of Multi-network SIMs and Multi-IMSI SIMs. The company makes extensive use of embedded SIM technology and has developed a range of SIM applets. In addition there is a research and innovation team whose focus is on improving the coverage, reliability, and security of IoT projects from within the SIM Card.

That focus includes adding support for embedded SIMs in order to future-proof connectivity options. Currently, MNOs are only allowing access to their eSIM profiles, rather than their IMISIs. Therefore Pod eSIMs (which are compliant with the eUICC standards for IoT) come with a default Multi-IMSI profile in order to provide additional resilience. Whatever eSIM profile an MNO employs, if connectivity fails, Pod's Multi-IMSI failsafe profile will restore connectivity with all the configured IMSIs.

In addition, the company provides "eSIM updates", e.g. when the eSIM profile is updated to improve security. They are packaged, downloaded remotely and activated as a new profile, enabling services to be rolled forward and back.

Multi-network SIM cards

The company's agreements with the leading network providers enables global roaming for one flat rate. These cards automatically change to another network in patchy coverage areas in order to connect to the strongest available signal.

Multi-IMSI SIM cards

An IMSI (International Mobile Subscriber Identity) is assigned to one operator and therefore provides one connectivity option. Every IMSI on Pod's Multi-IMSI SIM cards operates on a separate network infrastructure. Therefore if there is a connectivity issue the SIM automatically switches in order to obtain a better signal via a completely different architecture. Multi-IMSI connectivity is ideal for applications that need multiple redundancies to avoid downtime. For example, logistics and tracking where the device is in constant motion, often in rural areas and crossing borders. Multi-IMSI SIMs also provide additional resilience for mission critical applications such as emergency services or healthcare, which require real-time data transmission.

eUICC software

eUICC (embedded Universal Integrated Circuit Card) technology restructures SIMs. It provides multiple profiles on one card, which can be provisioned over the air (OTA). When eUICC is combined with Pod's Multi-IMSI the result is uninterrupted connectivity, cost-effective resilience and future-proof device connectivity.

With Pod's Multi-IMSI eSIMs the device will continue to benefit from a failsafe core network infrastructure if the main network IMSI experiences technical issues. At the same time, whenever the eUICC operating system is updated with new security protocols, they can be deployed over-the-air as an eSIM profile. Third party MNO eSIM profiles can be added into Pod's eUICC ecosystem in order to ensure all that connectivity options will be available.

SIM applets

The research and innovation team has developed and will continue to develop a range of SIM applets that are designed to resolve specific connectivity issues that can arise in the field. Awareness of these issues and determining the requisite functionality comes from close working relationships with the company's customers. The result is additional improvements in coverage, reliability, and security.

FPLMN Watch SIM Applet

This applet can be used to prevent or allow devices to connect to specific networks. The list of forbidden networks can be controlled even when the IoT application has been deployed. The Forbidden PLMN (Public Land Mobile Network) list is stored on the SIM card. It was developed to address a real-world mobility issue, the need to speed up network selection by ignoring forbidden networks that the device has blocked access to. However, as the forbidden network list is maintained indefinitely without intervention, blocking a network today might cause issues in the future when that network may be required.

IMEI Locker SIM Applet

This innovative applet enables control of the list of authorized devices that can use the SIM card to register on the network. The SIM reads the IMEI and validates it to decide whether to allow network registration. If a SIM is removed from the device and re-inserted into an unauthorized device, this prevents unauthorised usage and ensures an additional security layer. It also allows tracking of individuals who steal removable SIMs from critical devices in order to obtain free connectivity and then return them.

Device SIM/eSIM Compatibility Applet

The functionality that controls eSIMs and SIM applets is derived from the "Proactive SIM" standard. IoT devices must implement this standard and provide a set of configurations in order to be compatible with SIM applets and eUICC SIM technology. This SIM applet automatically detects applet and eUICC SIM compatibility. The reporting mechanism is particularly useful for IoT device manufacturers: they can safely evaluate and select the optimum modem to benefit from all Pod SIM/eUICC SIM capabilities.

APN auto-config Applet

This applet configures the correct APN on the devices automatically, thereby eliminating the requirement for it to be done by manufacturers. When used in combination with Multi-IMSI SIMs it enables different IMSIs to have different APN settings. The applet handles the configuration each time a new IMSI is deployed.

Conclusions

Pod Group does not aim to be an end-to-end IoT solution provider, instead the company provides the building blocks that enable solutions providers to create and deploy robust IoT applications and get them quickly to market. This ability comes from the specialist knowledge and experience acquired by the Pod team over more than 20 years. Working closely with customers across multiple sectors has given the team in-depth insights into the problems encountered before, during and after the deployment of IoT solutions.

The services provided by the Pod IoT Suite modules are designed to remove barriers to the growth of the IoT market, e.g. market fragmentation. Moreover, the ability to future-proof the application's connectivity, the potential to scale globally and the capacity to quickly create, manage and bill new services that generate recurring revenue ensure the success of IoT projects from the start.

Pod Group's overriding objective is to become the leading agnostic connectivity provider. Both cellular (NB-IoT, CAT-M1) and non-cellular (SigFox, LoRa) are integrated into one platform and managed via one interface. The company provides connectivity with 600+ global networks, but more significant is the fact that customers are in control. They own their SIMs and can control networks and connectivity via one platform.

This focus on connectivity and the management of IoT data has resulted in the successful deployment of solutions across mainstream business sectors. For example: Transport and Logistics; Healthcare; Energy and the Environment; Retail and Emergency Services.