Why the device is critical to delivering resilient IoT connectivity.

How Eseye's differentiated approach ensures highly resilient near 100% connectivity for every IoT device, every time.

Go beyond

How Eseye's differentiated approach ensures highly resilient near 100% connectivity for every IoT device.

Resilient connectivity is more than just an eSIM

Enterprises want the freedom to deploy a single eSIM SKU IoT device globally and have complete confidence it will always be connected regardless of the different levels of network availability across geographies, various regulatory environments, the complexity around permanent roaming or the technical issues caused by network outages.

At Eseye, we solve these issues for our customers with our unique architectural approach of interconnects and local breakouts with 25 global MNOs, our cloud-native Infinity platform and our **AnyNet+ SIM** which has been awarded 'world's best eSIM solution' three years running.[1]

The net effect is that Eseye customers with well-designed devices report 100% of data is delivered within specified latency. We believe this is the highest in the IoT industry and a significant factor in why Eseye has been successful in winning and deploying so many IoT projects for major global brands.

Since 2007 Eseye has implemented IoT projects for over 1,000 customers. Most of these customers came to us having already deployed their IoT project locally with an alternative supplier but then experienced significant issues when they attempted to deploy the solution nationally or internationally.

> "Since 2007 Eseye has implemented IoT projects for over 1,000 customers."

Our analysis of the root cause has shown that 80% of these issues were device related. Customers often believe that IoT connectivity is all about the SIM and the platform and as a result underestimate the importance of a properly configured IoT device. This is backed up by Gartner's assertion that "80% of IoT projects fail before they are deployed".[2]

Eseye insight. Once intelligent connectivity is integrated and optimised, our team will help you achieve near-100% uptime.

1 https://www.prnewswire.co.uk/news-releases/eseye-named-the-1-champion-esim-connectivity-provider-301986378.html
2 https://cio.economictimes.indiatimes.com/news/internet-of-things/8-out-of-10-iot-projects-fail-even-before-they-are-launched/52448887

To ensure IoT success, Eseye recommends that a series of technical tests for both connectivity and resilience are carried out on the customer's device as part of the initial testing and evaluation process prior to project deployment. These include, but are not limited to, the following:

- **The device can quickly switch** to another network if and when the device is in a location that does not offer connection to the original network.
- **The device can switch** to another MNO if there is a network error preventing data transmission to the last network it was connected to.
- **New IMSIs can be transferred** OTA into the device, especially for locations or countries where specific operator connectivity is required.
- **The device, if battery powered,** can take the appropriate action to optimize connectivity sessions so that the battery life is extended.
- **The device can localize a connectio**n onto a chosen network if necessary to avoid permanent roaming restrictions or reduce latency.
- **The device firmware** has been optimized to recover from any technical issues that cause cellular connectivity to be lost, temporarily or permanently (stranded assets).
- **That, if a future path to SGP.32** is needed, the device is technically enabled to transition to this new standard.
- **All of the above** are optimized to limit the likelihood that future changes to the Telecom landscape and regulations do not cause additional connectivity problems. These can include new permanent roaming restrictions around the world or requirements for compliance to country and industry specific legislation such as data sovereignty, GDPR, HIPAA and PCI.

> "Unless a rigorous testing process is carried out, regardless of what SIM is in the device, there is a very high chance that the deployed device performance will be below the level required by the IoT use case."

Eseye insight. We see IoT differently. Starting with the device is the key to the success we achieve for our clients.

Eseye's three step process to check your device will perform.

Eseye has a three stage process to ensure that your device will reliably connect every time:

1. Device Assessment
2. Device Validation
3. Device Remediation

1 Device Assessment

When an opportunity is identified and the customer says they want to do a bench test 'Proof of Concept (PoC)' of Eseye's solution, we ship them some trial SIMs and also carry out a remote device assessment test which cycles through the most common device issues that can affect connectivity.

> "The process can be carried out in less than a day and is designed to ensure that the bench test PoC is successful. There is no charge for device assessment."

2 Device Validation

If the customer wants to proceed beyond an initial PoC, the next stage is a more detailed device validation process

to undertake the additional tests outlined previously. In this case, one of our Technical Consultants conducts a broader set of device tests against a predefined script of connectivity and resiliency scenarios. The output of this is a detailed report of the findings, which is then discussed with the customer. This ranks the issues into different categories such as:

- **Critical** – the device will not perform to spec without the change.
- **Strongly Recommended** – for maximum connectivity and resiliency.
- **Recommended** – will improve device performance but can be fixed later post deployment.
- **Future Risk Mitigation** – not critical today but could be in the future based on customer deployment plans.

Device Validation is carried out as a fixed cost Professional Services engagement per device.

3 Device Remediation

If the customer, or their device partner, has access to firmware expertise they can make the necessary firmware changes to address the issues identified in the device validation report and Eseye will rerun the automated tests. If not, Eseye can carry out the device remediation and firmware updates via our in-house engineering team. This may require us to get permission to access the customer's device firmware source code.

Device remediation is charged as a variable fee depending on the project scope.

Eseye insight. With deep device and connectivity engineering expertise, we work in close partnership with our clients' teams, to build custom strategies.

Using AnyNet SMARTconnect™ to improve device connectivity resilience.

In response to customer requests to increase the overall resiliency of their devices when deployed, Eseye has developed AnyNet SMARTconnect™. This has two primary use cases:

- **Customers who are designing a new device.**
- **Customers who want their device to be able to switch IMSI without the need to communicate with the Cloud Management Platform i.e. enhanced device connectivity resilience.**

New device design capabilities

SMARTconnect is a lightweight device resident connectivity application which delivers three high level capabilities:

A. Management of the interface between the Eseye SIM and the modem.

B. The provision of a Firmware Over-The-Air (FOTA) capability for software updates to the modem, the application and SMARTconnect itself.

C. The management of the transmission of data from the device to the chosen cloud.

1. Managing the interface between the Eseye SIM and the modem

Encapsulated within SMARTconnect is a library of pre-coded modem commands built by Eseye to present instructions to the modem in the correct format. These pre-coded modem commands resolve the majority of the connectivity issues we have previously identified and remediated across our global customer base. Essentially these are a catalogued collection of lessons learned. By building these library APIs into the device firmware, we have found it reduces the need by 80% for customers to code this functionality themselves.

2. FOTA functionality

Device resiliency is not just affected by connectivity success. IoT devices can fail if the modem software is not up to date or if there is an essential update to the application that has not been installed.

SMARTconnect contains a capability for FOTA updates to the modem, the application and to download new functionality into SMARTconnect itself.

3. Device to Cloud data transmission

SMARTconnect enables data to be easily ingested into the cloud. The required data format reconfiguration for the chosen cloud provider is automatically set based on a service endpoint URL, including the certificate handling. An MQTT protocol stack is available for data transport so raw data can be delivered for SMARTconnect to format the data and deliver it into the cloud using MQTT.

Intelligent IMSI switching

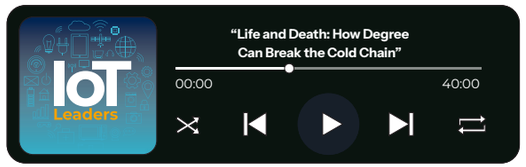
For new and existing devices where the customer wants enhanced resilience over and above the current connectivity levels, SMARTconnect enables the device to switch IMSI or select an alternative eUICC profile (either SGP.02 or SGP.32) when there is a network issue based on specific criteria.

For example, if a device is connected to a cell tower but a network outage means no data path is available, the modem will believe that it is still connected and so will the Connectivity Management Platform, and so no action will be taken to resolve the issue. This can lead to long periods without connectivity until the data path is re-established and potentially a further wait due to the signalling storm from thousands of attempted reconnections.

SMARTconnect can resolve this as it can be configured to conduct end-to-end network tests on a use case defined cadence and if no data path is detected it will execute an IMSI rotation to another profile already embedded in the SIM.

It will then work with the modem and the SIM to reset the current connection to check if this allows the data to flow.

For an example of this in action, click below to listen to the IoT Leaders Podcast with our US Healthcare customer PharmaWatch:



It is important to note this is not a user triggered capability, as this runs the risk of customers inadvertently selecting incompatible IMSIs within the SIM that degrade rather than enhance the service. Eseye will enable this capability as part of our managed service once we have worked with the customer to implement SMARTconnect into the device.

SMARTconnect is currently available as a SKU by modem type (e.g. Quectel BG95). By the start of 2025 it will be ported to the micro controller level to enable modem independence, Multi-RAT and more rapid development of value added extensions. This will mean that it can be rapidly scaled across a much larger range IoT device and modem configurations.

SMARTconnect is charged either as a SaaS fee per device or as a one-time license.

Eseye insight. With our expertise, we integrate, manage and optimise IoT device connectivity for estates of any scale or complexity.

Summary of how you can benefit from the SMARTconnect™ approach:

You do not need to have extensive firmware expertise and deep knowledge of cellular device connectivity. SMARTconnect codifies our extensive device experience in solving connectivity issues for hundreds of customers into an OTA installable in-device application.

SMARTconnect improves device resilience. The software can be configured to enable Eseye to allow the device to switch network provider without needing to communicate with the Connectivity Management Platform in cases when a network outage occurs.

SMARTconnect can manage OTA firmware updates. Further enhancing resilience by keeping the modem and application firmware up to date and by downloading new connectivity enhancements to the device as needed.

Automating remediation via software saves time and money. SMARTconnect transforms the remediation process from reactive (it's broken so I'll raise a ticket) to proactive (it looks like that it might break so the device takes action to remediate) and pre-emptive (your device will not break in the first place as all the firmware is up to date).

Built-in resiliency helps future proof the device from changes. With permanent roaming agreements and regulatory landscapes changing frequently, having a dynamic OTA and customizable connectivity solution helps to future proof the device and reduces maintenance costs and the risk of device downtime.

You can concentrate your focus. Direct your efforts on developing and deploying your IoT application rather than having to be device, firmware and telecom experts.

Build resilience into your IoT device

Contact an IoT specialist

Eseye insight. AnyNet SMARTconnect™ works with the modem and eSIM to select, manage and optimise the Radio Access Type (RAT) and network provider.


eseye
Go beyond
Talk to Eseye about
your **IoT journey** today.
Contact Us
Eseye
www.eseye.com