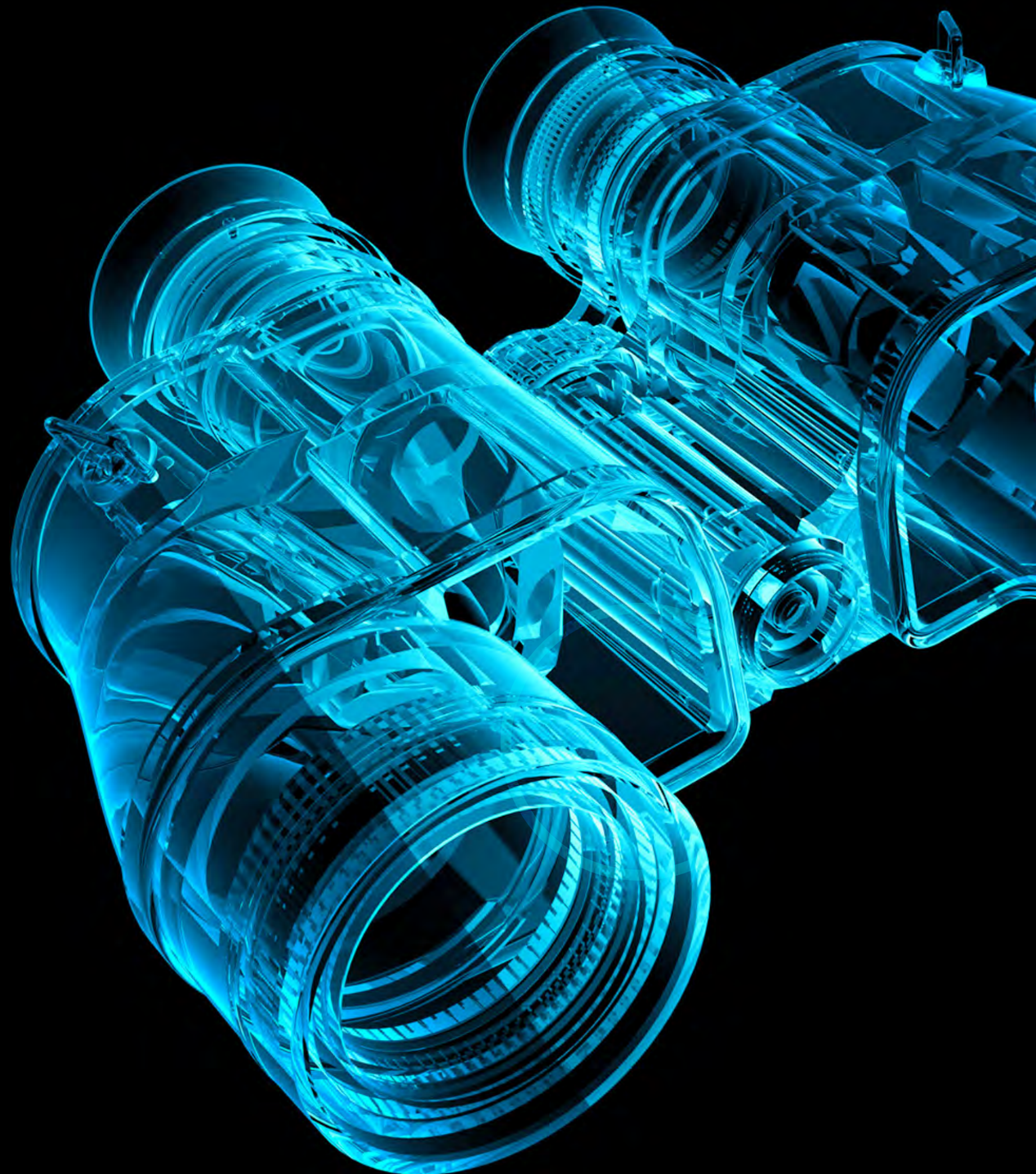
IoT Guide for Solution Architects

See IoT Differently

Designing cellular **IoT solutions** to work right first time, anywhere in the world.



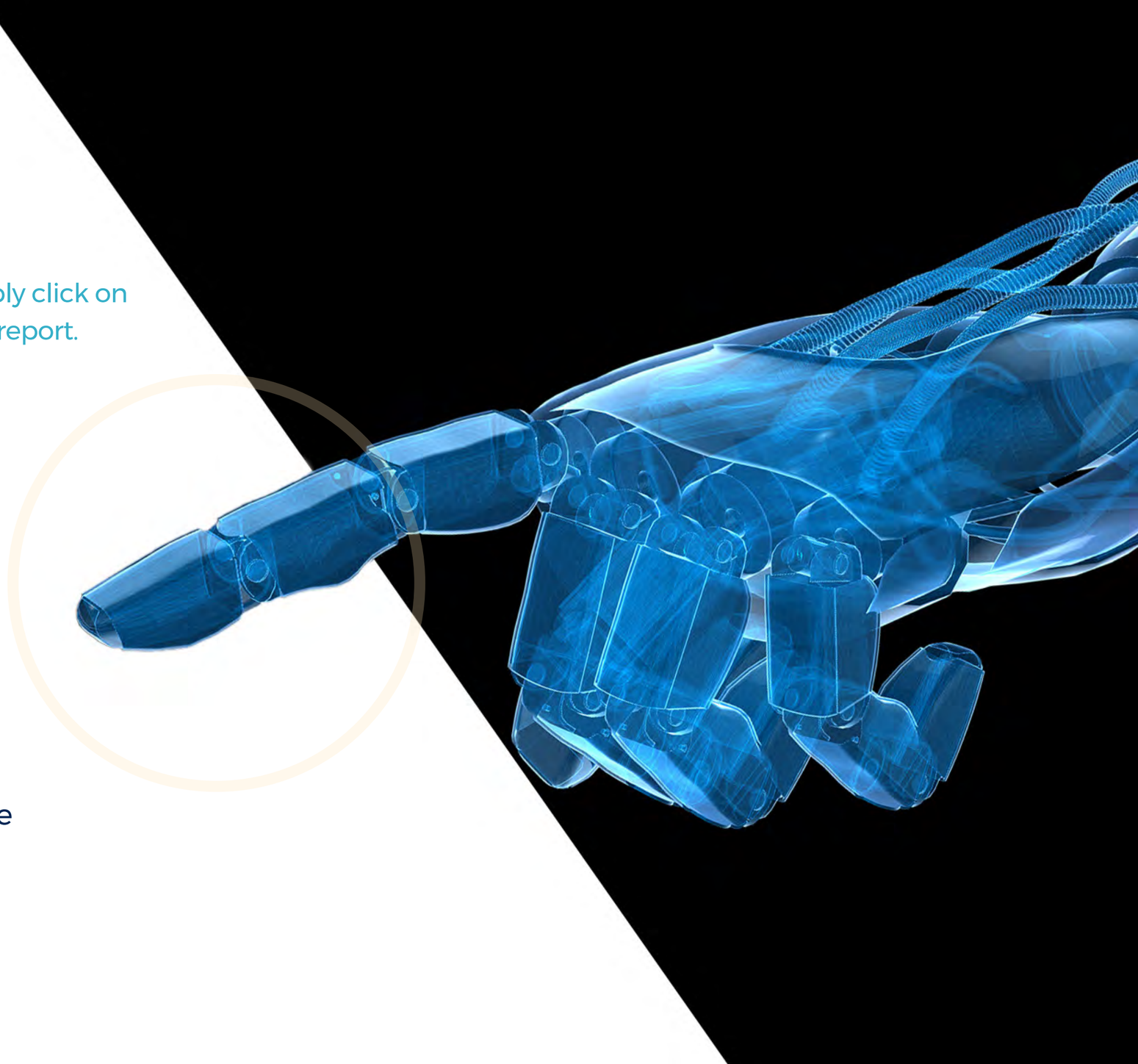
IoT Guide for Solution Architects
October 2021

Ref no: 9054

Contents

To view / jump to specific section, simply click on the icons below – and throughout the report.

Click on this icon throughout the report for additional information and data.



Introduction

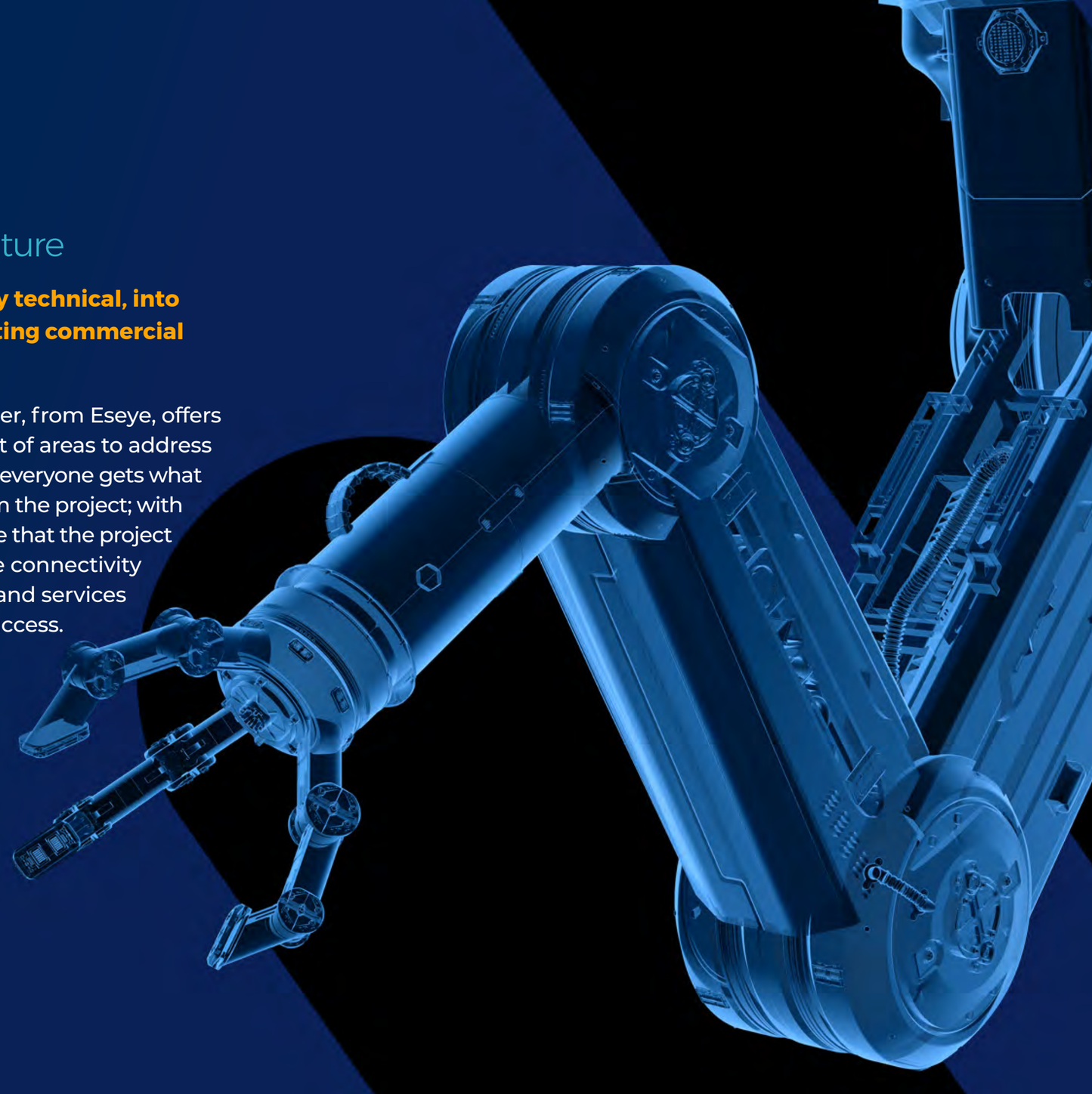
Architect the solution, define the future

The role of the solution architect extends beyond the purely technical, into a holistic and strategic approach which adds value by meeting commercial as well as technical objectives:

- **Inspiring confidence** among stakeholders, ensuring scalability and creating a sustainable strategy for the long-term (5 to 10 years).
- **Dealing** with localised operational challenges, and issues around roaming, protocols, and connectivity.
- **Bringing the business** case to realisation by interpreting its requirements while verifying best practice across the component parts of the solution.

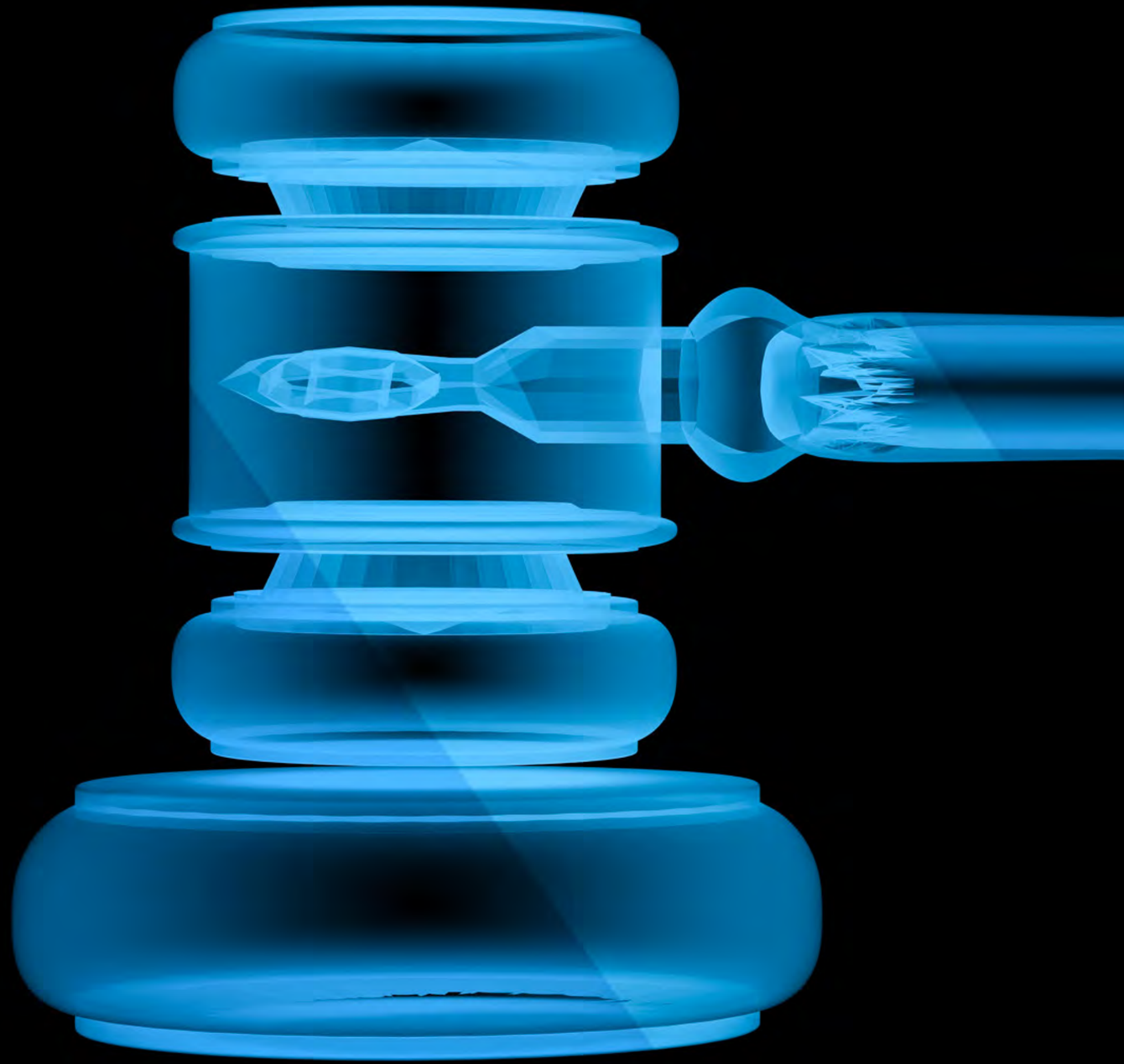
The solution architect provides an advisory perspective across all project factors such as coverage, availability, latency, global connectivity, sensor software, power supply systems and configuration of the SIM toolkit, data analytics, and security.

This whitepaper, from Eseye, offers you a checklist of areas to address to ensure that everyone gets what they want from the project; with the confidence that the project will deliver the connectivity performance and services essential to success.



Interrogate

See IoT Differently



Interrogate the business case – ensuring value, precision, and confidence.

All eyes are on the solutions architect to deliver on the business case.

IoT is *driving digital* transformation. As a solutions architect, you are inevitably tasked with making the vision for the solution a reality. In your role you are providing project assurance; managing quality, change, and risks in IoT projects to meet expectations.

To ensure you start your project on the right track – **you need to be interrogating the business case to understand** what functionality and level of device uptime are required. The answers to this then inform the key requirements you will need from your connectivity, platform, and hardware.

It will also help ensure that critical requirements are not 'cost managed' out of the solution later by your procurement team.

1. **What** existing solutions do you want to integrate this with and why?
2. **How** business-critical is the uptime of the devices?
3. **Where** are you intending to deploy solutions now and in the future?
4. **What** does the future solution roadmap look like and will this require new versions of your device, or can you achieve this with over-the-air software updates?

Your first step should be to understand your likely stakeholder group and their viewpoints on the outcome.

Some important stakeholders to consider:

CTO

Your CTO is looking at the solution you are creating from a viewpoint that balances the strategic needs of the business with the technical requirements, such as architecture, performance, and security. Ultimately their **approval is fundamental.**

For the CTO to approve your IoT design, specific requirements to meet include:

1. **Performance.** That the devices fulfil the brief and work as intended in all markets with the ability to scale and interoperate/integrate with existing and planned applications and systems.
2. **Futureproofing:** That the devices can be upgraded and will function universally with in the changing connectivity landscape and the technology stack.
3. **Cost rationale:** Assurance that the project is achievable within budget and incorporates the flexibility to accommodate future cost increases.
4. **Resourcing:** Full visibility of the team management and resourcing requirements to ensure a sustainable solution.

Some important stakeholders to consider:

CFO

The CFO will be looking to not only make a return on investment, most easily leveraged by reducing the investment but also generate revenue from new streams. For example, launching new products or experiences in new markets with IoT.

For the CFO to approve the IoT project, it is for the solution architect to change the context of the conversation and elevate it to the benefits to be gained from:

1 **Process simplification:** A single global device stock-keeping unit (SKU) will streamline manufacturing and supply chain processes, improving inventory management workflows and reducing inventory carrying costs.

A single **global eSIM** offering over-the-air updates simplifies the process of deploying to multiple regions, avoiding the need for hundreds of contracts with network operators and the associated costs and admin.

2 **Outsourcing:** of non-core activities which, across multiple geographies can bring a huge cost implication.

CIO/CISO

Requirements from the technology, data architecture, information management, and data security perspectives will include:

1 **Security:** How do you ensure that edge devices are not vulnerable or will not compromise the IT infrastructure in any way. You must consider how to manage device inventory security, risk assessment threat detection, and response protocol in the event of a malicious attack.

"You must consider how to manage device inventory security, risk assessment threat detection, and response protocol..."

2 **Cloud vs on-premises:** Are the devices integrating into existing infrastructure?

3 **Supporting these devices:** What resources will be required from their team to support these?

Some important stakeholders to consider:

Procurement

Procurement will be scrutinising every opportunity to reduce costs on a line-by-line basis. Guidance from the solution architect is essential in this sensitive area; clarifying that procurement specifies an RFQ that does not strip out key performance aspects.

They are not candidates for short-cuts or lowest prices, either of which tactics could compromise the success of the IoT solution.

Focus more on the attainment of key strategic gains:

1. **Freedom:** Avoid being locked into connectivity contracts.

"Guidance from the solution architect is essential in this sensitive area..."

2. **Flexibility:** Procurement stakeholders want the option to re-evaluate partnerships, providers, and contract frameworks regularly.

Product Development

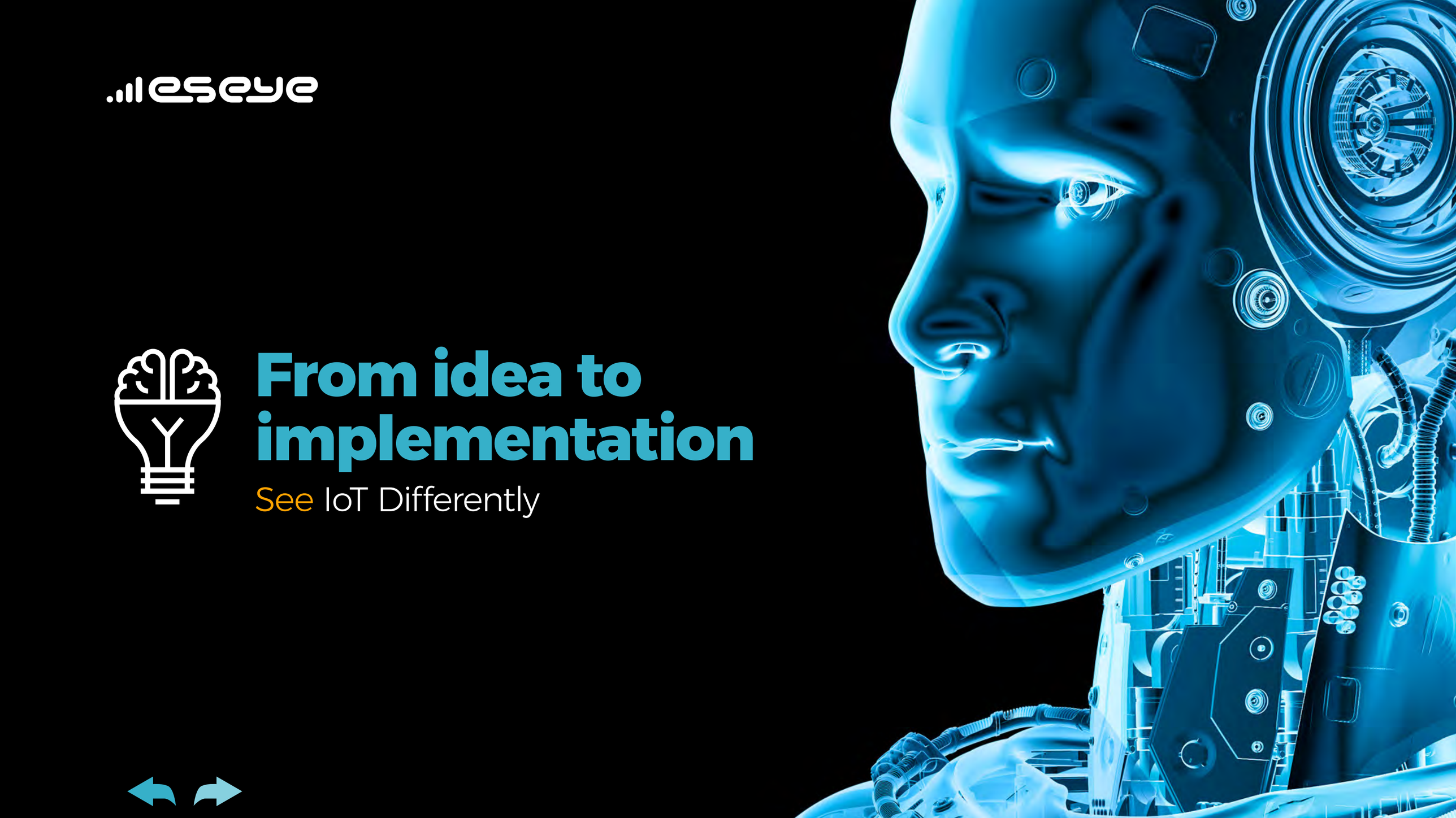
Product development concerns will centre on an understanding of the solution roadmap following deployment:

1. **Technical reassurance:** Will the device connect in each location identified for its deployment?
2. **Sustainable business value:** Will it deliver the business benefits, achieve the objectives, and support anticipated business growth?
3. **Future flexibility:** Will the product or solution need updates or upgrades? Can these be made over-the-air?

"...will centre on an understanding of the solution roadmap..."

From idea to implementation

See IoT Differently



Device design, onboarding, and certification

From idea to implementation

Designing the device

The device and its sensors are the data exchange hub, and one of the biggest time-sensitive parts of the overall project not least because it is the start point, but also because device development can commonly take between 12 and 18 months. Your IoT device and its multitude of sensors is the critical point at which data arrives; where you can sift, shift, and extract it to make sense of real-time information relating to user interactions and machine performance, whatever the machine may be; driving value and delivering better outcomes. The device is basically your boarding card.

During this stage, you'll want to consider standardising and simplifying production and deployment and ask:

- **What** type of data do you want to collect? This will influence sensor requirements.
- **What's** the purpose of the device? What is it built to do and achieve?
- **How** will it connect? And how will you manage device connectivity?
- **Where** will it be used? What geographies will the device be active in, will it move or be stationary? The best practice is to design the device as a single SKU.

"Ultimately you will need to assess internal resources and capabilities and determine if it would be timelier to bring in outside expertise to help you build your solution and ensures it is ready to be connected from the start – avoiding costly delays to your project"

IoT edge hardware – build vs buy

One question that frequently arises is whether to build or buy IoT hardware. Enterprises are increasingly exploring the build option and looking to create their own SM-SR (Subscription Manager Secure Routing) system and core network connectivity platform.

Alternatively, a Build-Operate-Transfer (BOT) model enables enterprises to work with an expert connectivity provider to build the SM-SR and platform, and gain insight and skills on how to operate it.

Onboarding the device

At this stage, you should ensure that your device is performing as expected and is ready to contend with any unforeseen challenge. **80% of IoT projects fail due to an issue at the device level,** so it's vital that your device is **extensively tested** so it's prepared for a lifetime in the field. There are three critical onboarding tests when looking to secure this outcome:

- **Network logs.** Ensuring that the device is communicating correctly; no unexpected traffic to drive up the connectivity cost or put the device at risk of a security breach.
- **Test commands.** Providing reassurance that the tools you deploy will successfully manage the connectivity service for years to come.
- **Device testing.** Test the device in a controlled environment by causing a disruption of service and creating unusual error conditions.

Again, you need to look at your expertise within your team and assess if you have these as in house capabilities. Due to onboarding cellular devices being a niche skill it may be worth investing in outside support to ensure your solution functions as intended.

IoT protocols

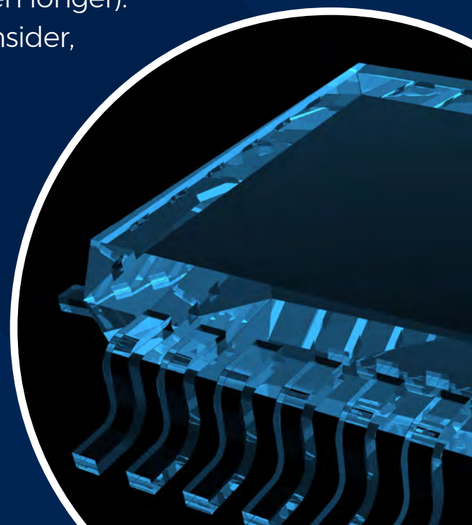
IoT protocols enable hardware to exchange data, and they should be tested during the onboarding stage, to ensure that your device can recover in such situations. As with any aspect of the project, this apparently simple solution comes with its own complications in that there are no standardised IoT protocols.

"...this apparently simple solution comes with its own complications..."

The best approach is to consider all the protocols your device will need for the long-term (10-15 years or even longer). For the extensive range of protocols you need to consider,

see Eseye's Ultimate Buyer's Guide to IoT.

"The best approach is to consider all the protocols...



Certification considerations

Without certification, your device won't make it far from the lab bench. Unfortunately, it's not as simple as conforming to one set of standards and your device is good to go. More likely your IoT device will need multiple regulatory certifications depending on which markets and countries you wish to deploy to.

Three types of certification must be considered:

- **Regulatory:** before products can be sold in specific markets, they'll need to comply with standards such as electrical safety and Radio Frequency (RF) emissions interference.
- **Industry:** the telecoms industry has two main certification schemes – the Global Certification Forum and PTCRB. Network operators often require one of these schemes to be obtained as part of acceptance or certification requirements.
- **Operator:** some mobile network operators run testing and certification schemes to minimize connectivity issues and ensure the network is used appropriately by all users.

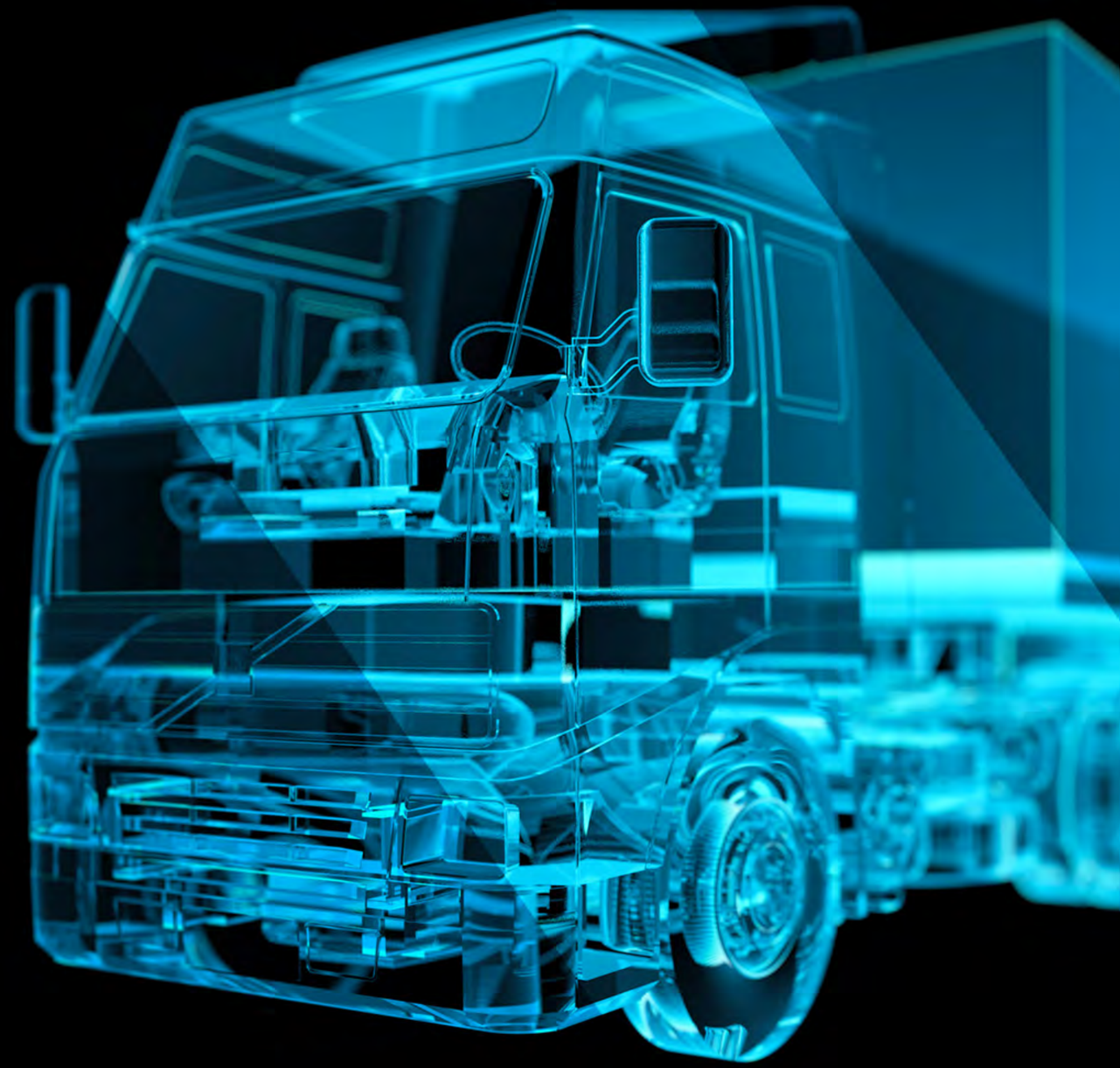
Getting past this stage in an IoT project is undoubtedly one of the most challenging. It requires extensive knowledge, plenty of time and resources, and for you to be heavily involved and aware of all the moving parts – from protocols to certification to security and more!

For more information, read Eseye's Getting Started: IoT Device Onboarding and Deployment whitepaper.

> "Fortunately, Eseye has been there before and offers consultancy at each crucial step. By leveraging our technical expertise, we can minimise risk and set your project up for success.

The IoT Ecosystem

See IoT Differently



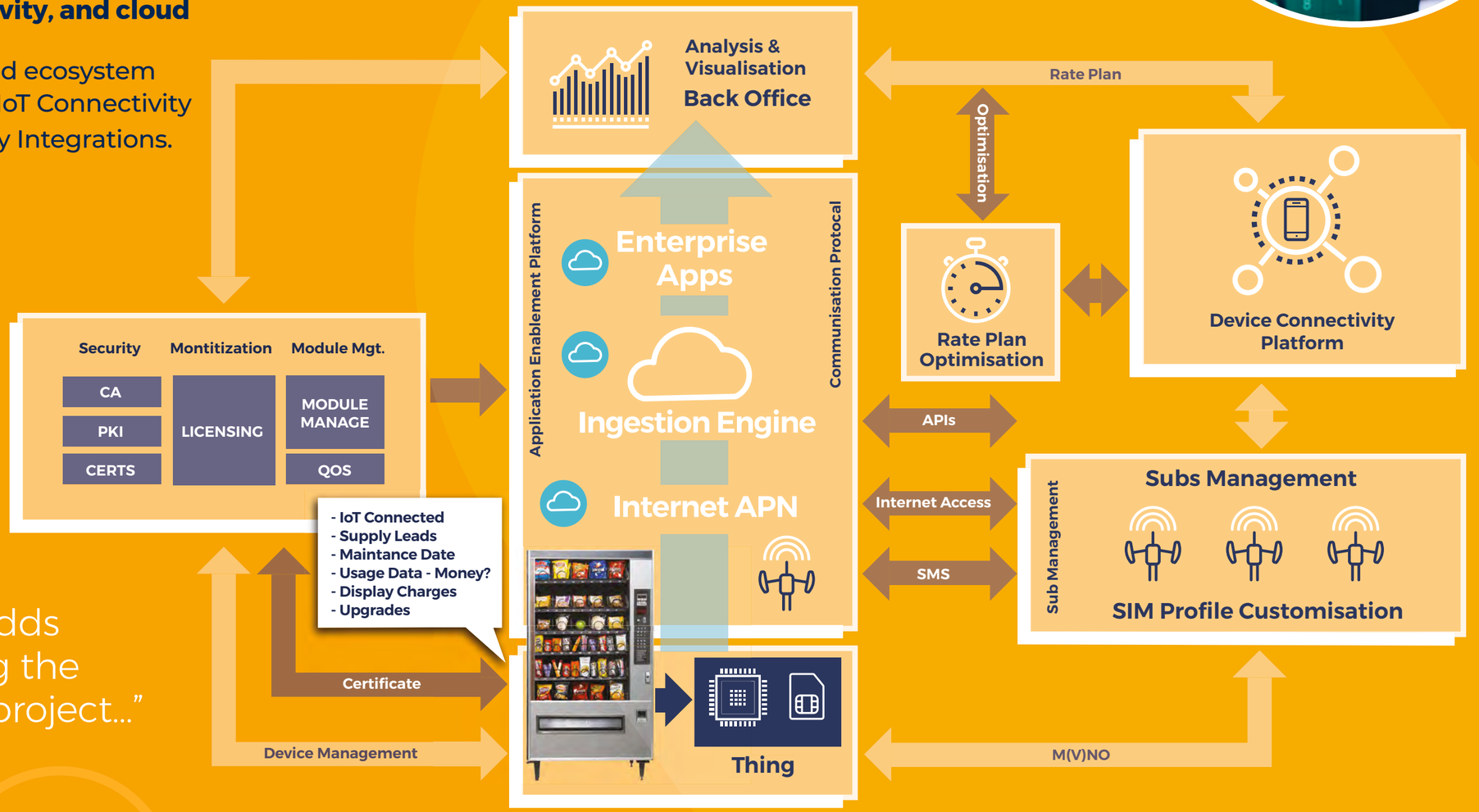
The IoT ecosystem

Technology integrations, connectivity, and cloud

The complexity of the IoT fragmented ecosystem brings challenges in multiple areas: IoT Connectivity | Cloud Integration | API / Technology Integrations.

It is not uncommon for the finance function to evaluate components of an IoT project in isolation. They may evaluate the component costs and how they reflect on the project investment on a country-by-country basis. Instances such as this are where the solution architect adds value through envisioning the potential lifecycle of the project, **offering a future-proofing benefit projection to clarify matters for finance.**

"...the solution architect adds value through envisioning the potential lifecycle of the project..."



Three foundations to your IoT solution

1. IoT connectivity

Key considerations

Connectivity is the backbone of all that your project sets out to achieve, across a potentially widely dispersed estate – the services you will be delivering and the data that will be constantly flowing through the system.

You will need to ensure as close to 100% uptime as possible, managing a web of mobile network operators (MNOs). This is a complex and costly task, and often a waste of effort for an organisation working as one single entity; unable to access the economies of scale available to larger providers of IoT connectivity.

In addition, should you wish to change network operators, challenges arise with migration. Integrations between the new operator's infrastructure and the eSIM platform must be made before any switch can take place, which often takes months and can cost hundreds of thousands of dollars.[2]

Two solutions to gaining operational efficiency will remove the complexities:

A SIM card that allows for dynamic and seamless switching between network profiles and is fully eUICC*- compliant	A Connectivity Management Platform (CMP)
The SIM card should allow for dynamic (on SIM or over-the-air) and seamless switching between network profiles, while being fully eUICC and GSMA compliant. The SIM should offer multiple bootstraps (multi-IMSI) or network operator profiles: these permit a two-way interchange between the bootstrap and the eUICC step 2 profile (which localises the SIM to the network) to enable a fallback capability.	A connectivity management platform (CMP) is a single application allowing you to centrally control your global IoT deployment/s and streamline device administration. You can manage network connectivity for each device and change operators as required.

*Embedded Universal Integrated Circuit Card

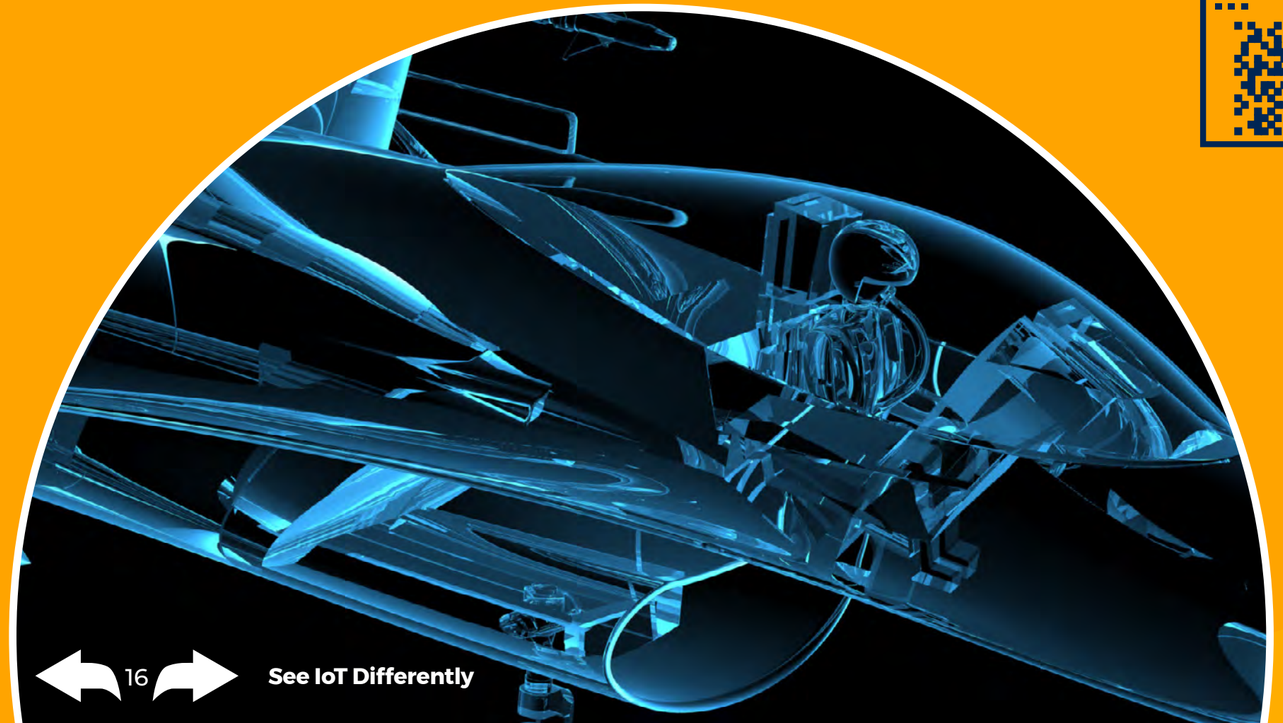
[2]Eseye and Kaleido Intelligence, Solving Permanent Roaming Challenges Through eSIM and Localisation Whitepaper

Three foundations to your IoT solution

2. Cloud providers

Key considerations

You will need to ensure the right cloud and analytics support to scale up as data volumes increase and variety becomes more complex. The cloud environment, and the cloud marketplace, address targeted usage requirements, across private, public, or hybrid and cloud utilisation.



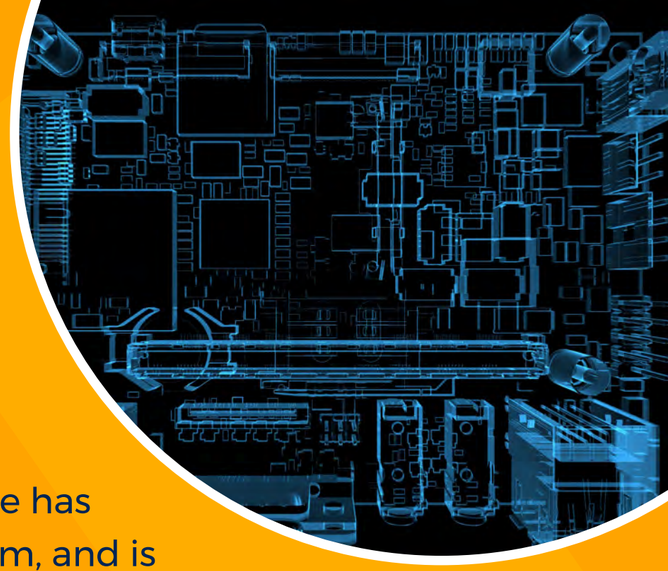
The main considerations are:

Secure and automated transfer of data to your private or public cloud platform and enterprise tools.

Data sovereignty and regulatory requirements: compliance with local data sovereignty requirements, while reducing any exposure to changes in attitude/regulations towards permanent roaming.

"You will need to ensure the right cloud and analytics support to scale up as data volumes increase and variety becomes more complex."

*Embedded Universal Integrated Circuit Card



Three foundations to your IoT solution

3. API / technology integrations

The route to other sources and greater value from your data lies in the deployment of the application programming interface(API).

This is a standard protocol for exchanging two-way information between systems and components, enabling the business to collect data from various sources in an automated and efficient way.

"This is a standard protocol for exchanging two-way information between systems."

Considering API integration from the very start of an IoT project will enable you to provide greater flexibility and choice of enterprise apps you may wish to interoperate with in the future. It future proofs your project, paving the way or connecting with and leveraging the value of other systems when the time is right.

*Embedded Universal Integrated Circuit Card

The main considerations are:

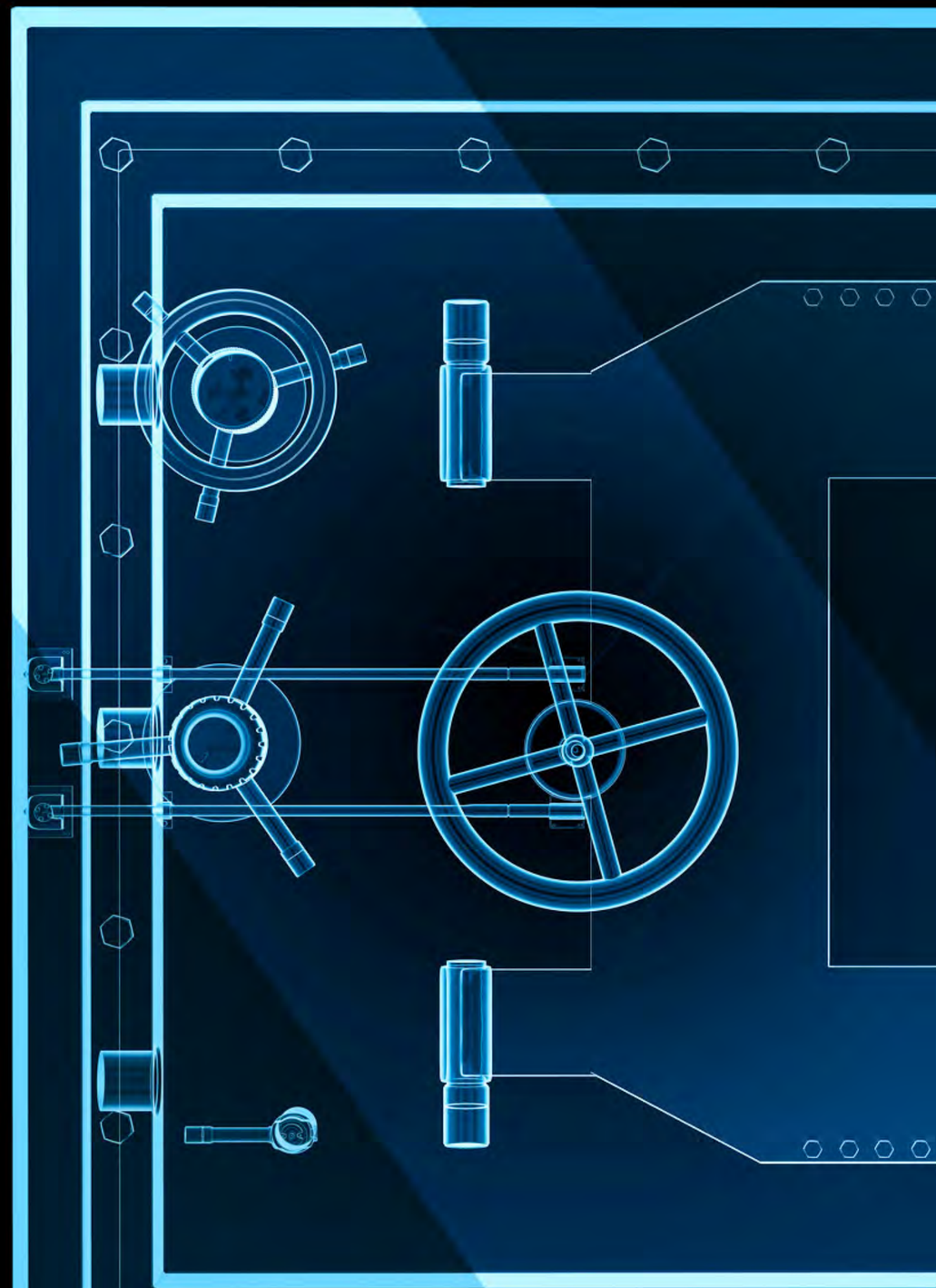
Data origin – where has the data come from, and is it secure?

Identify integration requirements – how can your data be enriched by other sources to deliver maximum business value?

Leverage the cloud – to make sense of it all and uncover more value, can your data be surfaced through an analytics platform or dashboard, where behaviour can be analysed, and deeper insight can be drawn.

Security

See IoT Differently

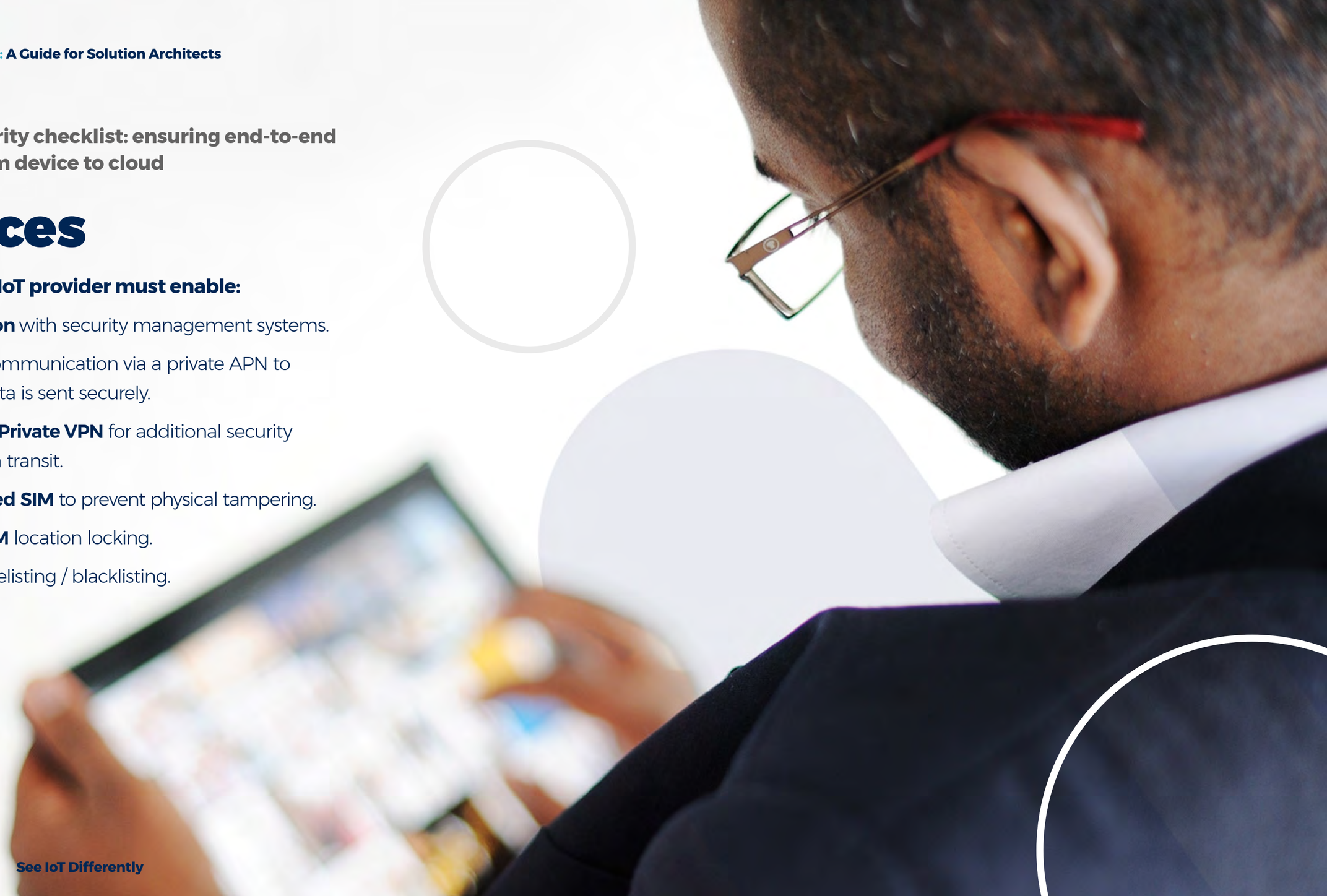


The IoT Security checklist: ensuring end-to-end security, from device to cloud

Devices

Your cellular IoT provider must enable:

- **Integration** with security management systems.
- **Secure** communication via a private APN to ensure data is sent securely.
- **Optional Private VPN** for additional security for data in transit.
- **Embedded SIM** to prevent physical tampering.
- **IMEI & SIM** location locking.
- **SMS** whitelisting / blacklisting.



eseye

The IoT Security checklist: ensuring end-to-end security, from device to cloud

Network

Your cellular IoT provider must have a private, secure APN to deliver:

- **Connection** authentication.
- **IP** address allocation.
- **Secure** data routing to a private or public Cloud.
- **Reduced** risk in using a standard shared MNO internet connection.
- **Monitoring** data on device activity and network usage.

As an additional measure, you could consider agentless security. Such a solution discovers and monitors all IoT devices in your estate, continuously assesses device vulnerabilities, risks, and policy violations, and automatically responds to anomalies that could put devices and your business at risk.

Learn about how to achieve agentless security for IoT devices on cellular networks.

ARMIS

Proof of Concept (PoC)

See IoT Differently

Proof of Concept (PoC)

The PoC stage is when stakeholders will be assessing the outcome from their perspectives; will it work, will it deliver, be secure, will it serve the business purpose at the costs identified, and will it bring in the required return on investment?

> Your IoT theory must be tested in its native environment, where real data can be gathered to support your operational planning and investment business case requirements.

You are looking to ascertain whether your devices behave predictably, connect consistently, and achieve business outcomes. Potential problems may be missed and unanticipated if you do not run a significant proof of concept.

- **Ecosystem ready?**

The best practice approach is to deploy a significant number of devices (e.g., 50) to test in the field, withthe selected SIM in place and with the requisite connectivity and support services.

- **Duration**

A short proof of concept will only prove the concept, not test the reality or long-term viability of your deployment. Your devices should be tested in situ for at least 2 months to get a real feel for how your devices will deal with challenges like permanent roaming and network/latency variance.

- **Processes ready?**

It further involves putting into place the relevant processes to enable scaled deployment. This may include testing at manufacturing, access to and setting up a connectivity management platform, SIM activation, SIM management billing and other processes unique to your solution requirements.

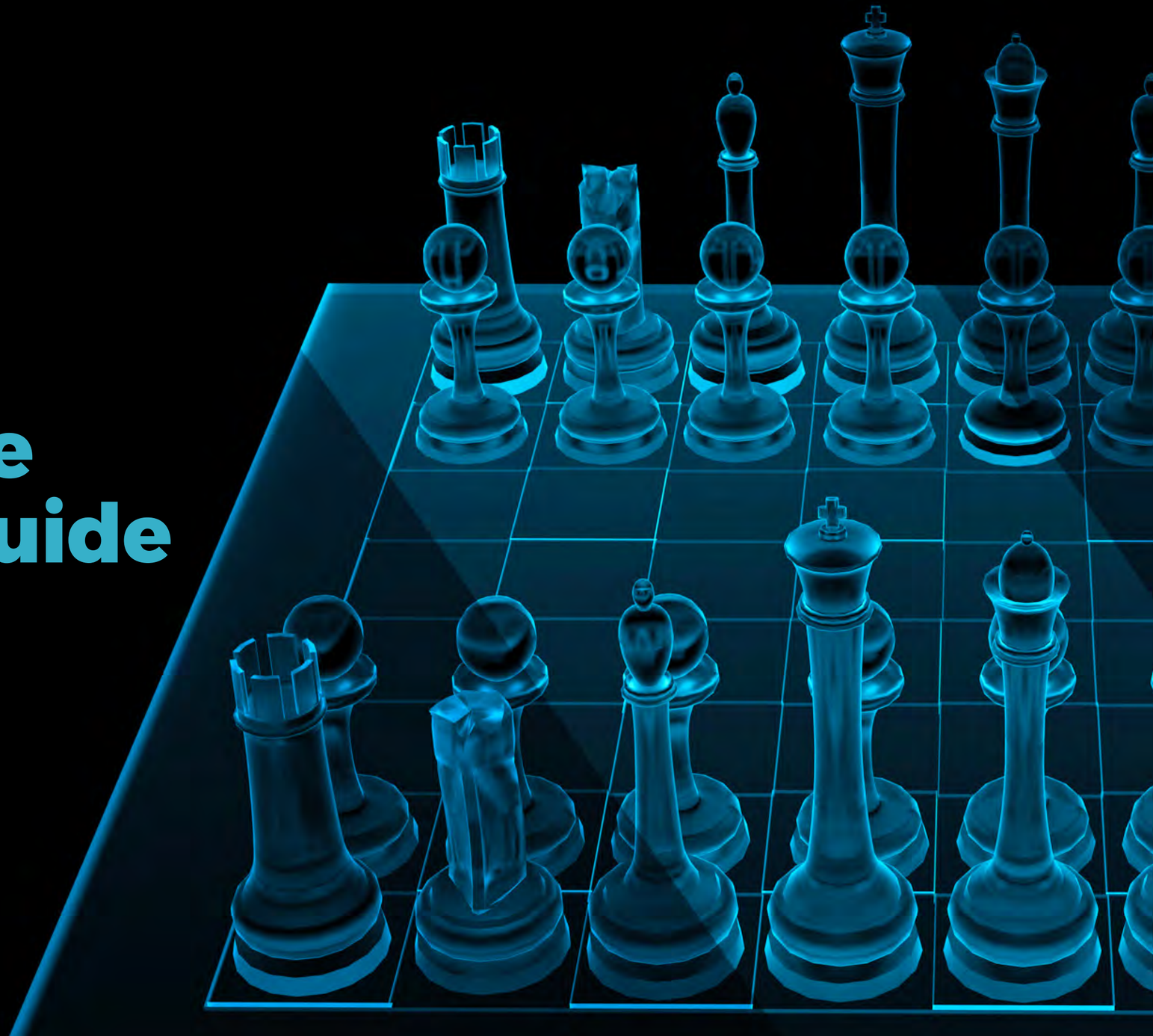
- **Fine-tuning done?**

The PoC will indicate what refinements to the technical solution may be needed to ensure optimal connectivity services for your devices.

"When these phases are completed, nothing stands between you and deployment."

Choose the right IoT guide

See IoT Differently



Choose the right IoT guide for the journey ahead

It's a **long journey** and with a potentially wide audience watching every step you take it can also be a complex one.

Tick the key boxes, and you're ready to go:

- ☑ **Get the device design right** and through to prototyping in the shortest time window, and you will have addressed concerns around budget.
- ☑ **Look closely at connectivity** and security and you will have satisfied those concerned with the operational validity and value of the solution.
- ☑ **Adopt a single SKU** approach and you will have satisfied many procurement concerns.
- ☑ **Test the device** and the solution in the field through a rigorous PoC.

At the outset of your project, you may well look for accomplished partners who can not only help you along the way but can be there for you when all is up and running.

Eseye can help you unlock the power of IoT. Combining hardware device engineering and technical know-how, our technical consultants and solution architects work collaboratively and proactively with you to identify and resolve any configuration issues before you move into full-scale production or extended field trials. Our unique Connectivity Management Platform enables devices to switch intelligently to any one of over 700 GSMA-compliant carriers to maximise uptime with near 100% uptime, across 190 countries.

Secure, universally available connectivity.

Eseye's intelligent patented network switching AnyNet technology helps organisations achieve near 100% universal connectivity for their IoT devices. These special partnerships enable customers to seamlessly switch from one operator profile to another, meaning that coverage blackspots are eliminated, and devices can be localised onto local networks. No other IoT connectivity provider has access to this unique network of interconnects or can offer a similar device localisation capability.

Ready to architect your IoT solution? Get in touch to speak with an IoT specialist.


No Limits.