consult.red
Connected Devices & Systems

From Zero to Hero: Scaling IoT
Product development playbook

// Deliver profitable, secure, smart products to market

58%
of IoT projects fail

With our help yours needn't be one of them

Beecham Research 2020

What we'll cover

Our 6-stage approach to rapidly achieving scale while managing technical and commercial risk

// **Stuart Griffin**

Co-founder & Chief Operating Officer
stuart.griffin@consult.red

// **Rahul Mehra**

Co-founder & Chief Technology Officer
rahul.mehra@consult.red

//consult.red

The challenge of scale

Avoiding the pitfalls of scaling your IoT Solution

According to Beecham Research 58% of those involved in both successful and unsuccessful IoT projects said that they had problems with scalability.

Successfully delivering a secure IoT product in volume takes experience, and in this dynamic market can mean make or break for your business.

Often, an IoT business model only works at scale. Yet, the technology and the market are both untested at volume. The true cost of investment and resource to achieve scale is often underestimated, as are the risks involved, leading to a loss in stakeholder confidence (and sometimes funding).

As a trusted technology development partner, we've developed smart, secure technology that's in over 30 million homes worldwide - we know what it takes to scale connected devices and systems. We've taken our customers from idea and concept to millions of deployed products; we know the journey. We help them manage risk, keep stakeholders on side and deliver successful, profitable products to market faster.

//consult.red

// Overcoming the IoT paradox

IoT business models need scale to achieve profitability, but risk will always be a factor

The collection and communication of personal data is essential to deliver the personalised IoT experiences that users want and expect. But, at the same time, users find IoT devices 'creepy' because they are collecting this personal data. Developers need to deliver versatile, interoperable and scalable IoT platforms, while also ensuring the security of personal user data - this is the IoT paradox.

There have been many predictions about the potential number of IoT devices that will be in circulation. Many have proved to be over-optimistic, perhaps underestimating the scale of the challenge.

Scaling your product to the hundreds, thousands or even millions brings additional commercial and technical risks that can be easily overlooked during development and early deployment. Getting your IoT product to scale profitably is a multi-stage journey that requires different skills, experience and approaches at each stage.

It's also a journey along which you'll have to make some tough choices – what we've coined 'trade-offs' – and peppered throughout this playbook are some critical decisions that we think you'll have to grapple with.

The good news is that with the right approach, the risks you face can be minimised.

Trade off #1
Partner vs develop in-house

Technologists often bring in a development partner, such as Consult Red, because they recognise it helps their in-house teams accelerate development.

Yes, bringing in outside help does mean an investment of time and resource upfront to bring teams together. Still, in our experience, that is more than offset by the benefits – avoiding pitfalls, broader experience across multiple technologies, (e.g., software, hardware, apps and cloud) and accelerated time to market. You're working with someone that's walked the path before, knows the risks and can help inform decision making.

There are also longer terms benefits; by working with the right partner, your team will benefit from knowledge transfer building their skills and capabilities without the downside of costly mistakes. It's fair to say that on some projects, we've engineered our redundancy by helping clients to recruit the right staff to carry on critical functions after transfer.
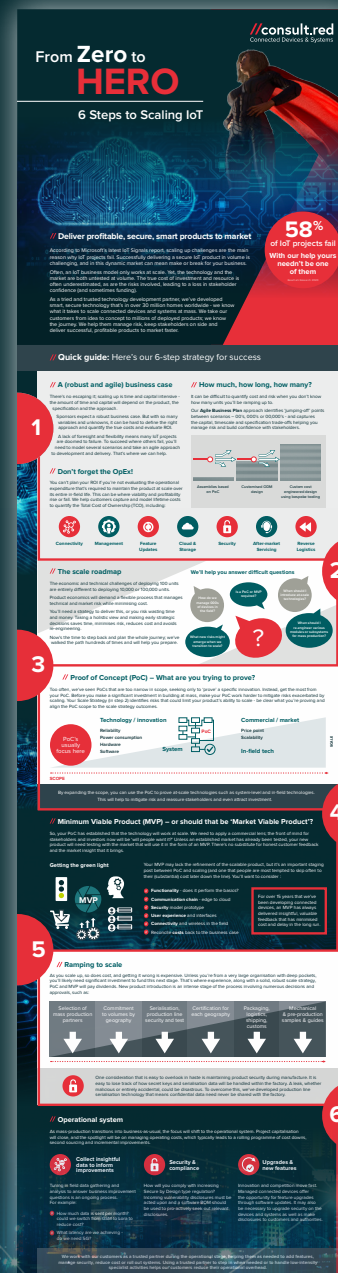
// consult.red

// Accelerating development

A closer look at the benefits of bringing in a partner

It's always possible to learn by doing and to develop your IoT product unaided.

The problem with this approach is that the way can be full of traps and involve going around in circles. Having a partner to guide the way can avoid pitfalls and facilitate your development's acceleration, letting you focus on your goals without repeating the same mistakes others have made and re-learning the path to scale.

Having a guide will help you navigate and overcome many complex challenges.

- Connected devices and systems, such as the Internet of Things (IoT), involve complex trade-offs across multiple technologies.

- From idea to proof of concept and scale, any roadmap is complicated by the availability of components and where and how to manufacture at scale.

- Secure by Design requires a security mindset that impacts choices at all stages of the journey. Realising the full ramifications of security at the end of a project can be extremely costly.

- Engaging early with all stages of the development journey prevents expensive changes down the road.

- Each stage of the journey introduces a new set of uncertainties.

- Working with a partner de-risks each step optimising the path to scale.

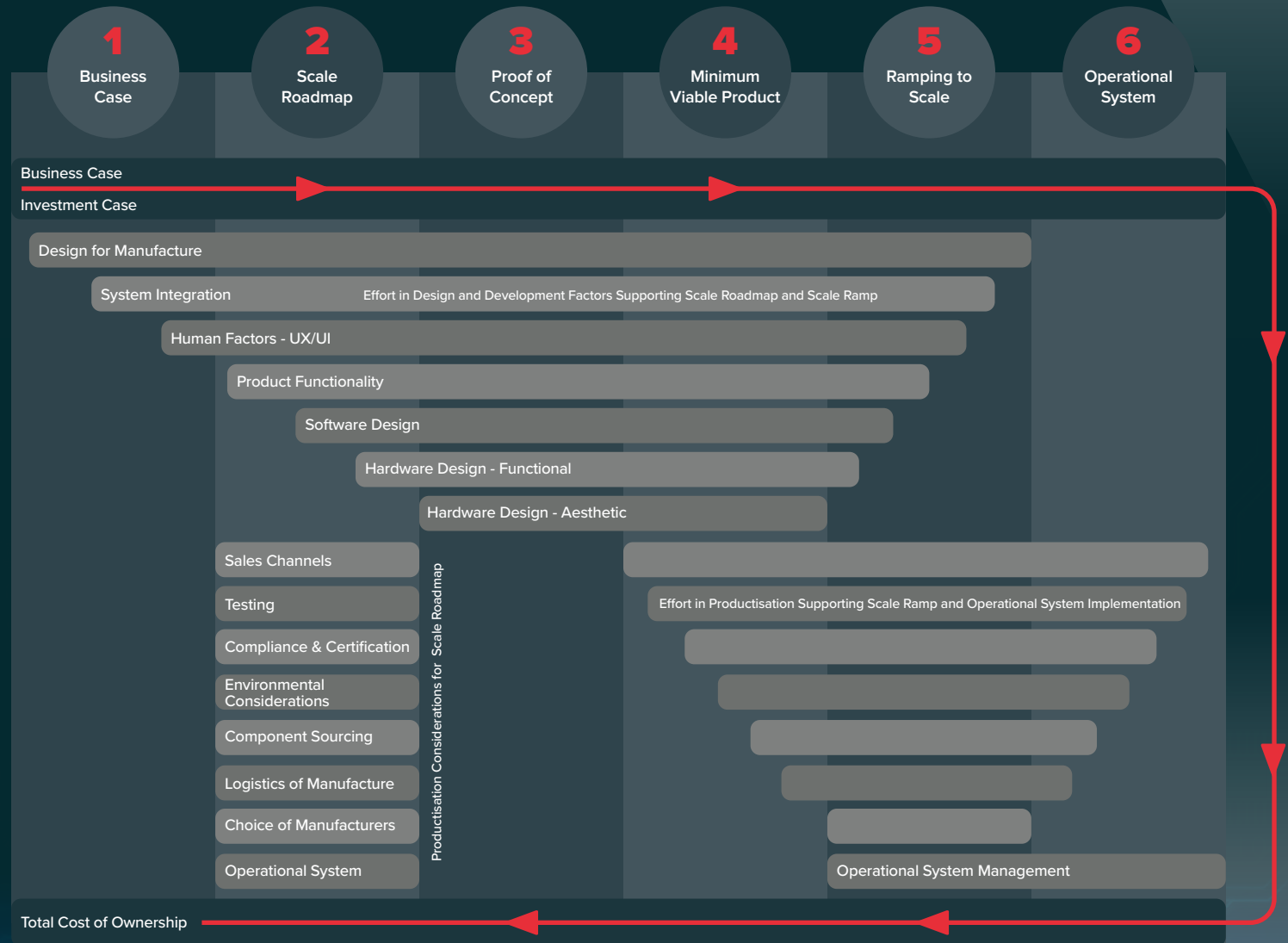//consult.red

// Going it alone?

What you'll need to think about and when

If you decide the right path is to develop your product without a partner, the graphic to the right might be a helpful guide. It outlines some of the key considerations at each stage of the product development journey.

Notice that the development of the business case - the first of our 6-stage journey - is ongoing. You'll want to keep cross-referencing and readdressing your business case as you go along. This, in turn, will have an impact on the total costs of ownership and ultimately how profitable your product is going to be for your business.

Studies have shown that an ill-defined business model is a significant source of failure among IoT projects.

The Scale Journey

1 Business Case
2 Scale Roadmap
3 Proof of Concept
4 Minimum Viable Product
5 Ramping to Scale
6 Operational System

Business Case

Investment Case

Design for Manufacture

System Integration — Effort in Design and Development Factors Supporting Scale Roadmap and Scale Ramp

Human Factors - UX/UI

Product Functionality

Software Design

Hardware Design - Functional

Hardware Design - Aesthetic

Sales Channels

Testing — Effort in Productisation Supporting Scale Ramp and Operational System Implementation

Compliance & Certification

Environmental Considerations

Component Sourcing

Logistics of Manufacture

Choice of Manufacturers

Operational System

Operational System Management

Productisation Considerations for Scale Roadmap

Total Cost of Ownership

// consult.red

// Business case

A robust and agile business case, considering Total Cost of Ownership (TCO) is fundamental

In 2022, global IoT spending is predicted to hit **$1 trillion**

* IDC, 2022

How much, how long, how many?

It can be difficult to quantify cost and risk when embarking on a staged approach to scale. A flexible approach to execution is needed to accommodate all the modelled scenarios.
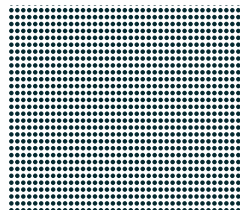
Agile business plan

Assemblies based on PoC

Customised ODM design

Custom cost engineered design using bespoke tooling

An agile business case identifies jumping-off points between scenarios and captures the capital, timescale and specification trade-offs. For instance, a deployment might start with 100s of assemblies based on the PoC, move to 1000s based on a customised ODM design before switching to 100,000s based on a custom cost engineered design using bespoke tooling.

Don't forget the OpEx!

You can't plan your ROI if you're not evaluating the operational expenditure that's required to maintain the product at scale over its entire in-field life. This can be where viability and profitability rise or fall. We help customers capture and model lifetime costs to quantify the Total Cost of Ownership (TCO), including:

Connectivity

Management

Feature Updates

Security

Cloud & Storage

After-market Servicing

Reverse Logistics

Our experience includes working with our customers to capture and model these lifetime costs to ensure they have a robust and agile business plan.

// consult.red

// Business case

Defendable business cases require practical understanding of many factors including scaling production and deployment

Considerations across the whole product and in-field lifecycle

Product

- ✓ Identify the outcomes that are sought and identify the benefits.
- ✓ Build the business model.
- ✓ Identify the data that is required to both implement the approach and to measure the benefits.
- ✓ Develop the proof of concept to scale roadmap.
- ✓ Use a security mindset to consider what the proportionate, scale security requirements are.

- ✓ Undertake a risk analysis of the options for implementation. Look for comparator and previous examples.
- ✓ Model the total cost of ownership of the complete system implementation.
- ✓ Does the business case answer what investment is needed and when? Not just unit cost feasibility.

Hardware

- ✓ Tooling costs, new product introduction costs and other NREs need to be considered – options for volume pricing.
- ✓ Important to consider hardware and mechanical costs and implications for volume manufacture. The cost of a hardware BOM changes dramatically with volume.
- ✓ Compliance & Certification costs – these can be geography specific.

- ✓ Need to understand volumes, ramp (factories specialise by volume i.e. <10K is small).
- ✓ Trade-off per unit cost vs internal capabilities (ODM will do more or less at a price/volume).
- ✓ Lead times, parts, shipping, FOB and tariffs, duties, (factors - where assembled, telecom devices).
- ✓ End of life for parts.
- ✓ Dual source, redundancy.

Software

- ✓ For software development non-recurring engineering (NRE) typically dominates cost.
- ✓ Important to consider hardware and mechanical costs and implications for volume manufacture. Hardware bill of materials (BOM).

- ✓ Need to consider SW operational costs – updates and device management (cloud service costs especially with data storage growth).
- ✓ Licensing and IP landscaping are essential to manage liabilities.

Operations

- ✓ Consider HW and mechanical costs and implications for volume manufacture. HW BOM.
- ✓ Reverse logistics - dealing with failures (maintenance & after sales).

- ✓ Deployment and installation costs.
- ✓ Maintaining and reporting - managing security vulnerabilities.

We have full life cycle experience and help clients to create business plans and TCO analysis
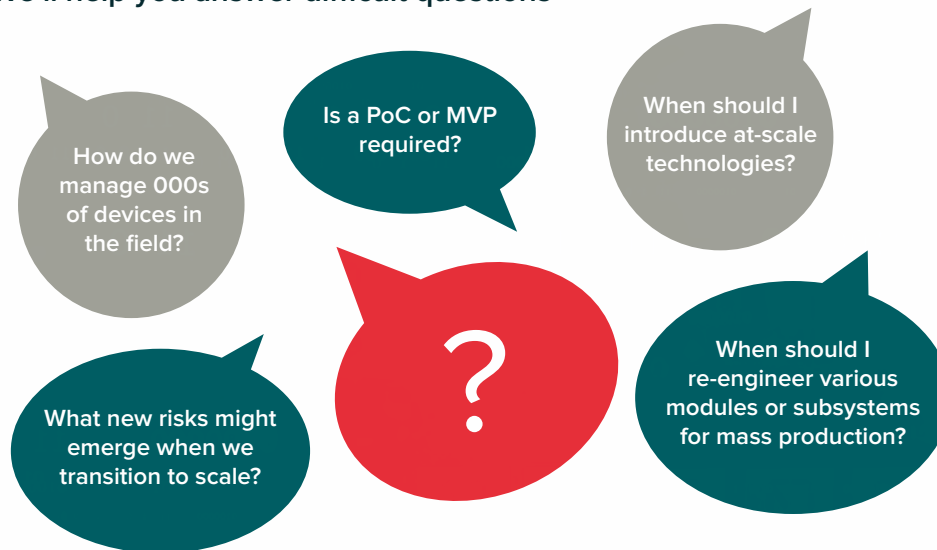
// consult.red

2

Developing a scale roadmap and a strategy will reduce the risk of wasting time and money later

The economic and technical challenges of deploying 100 units are entirely different to deploying 10,000 or 100,000 units. Having a clear roadmap appropriate to scale that manages risks while minimising cost is essential for success. You'll need a strategy to deliver this, or you risk wasting time and money. Taking a holistic view and making early strategic decisions saves time, minimises risk, reduces cost and avoids re-engineering.

Now's the time to step back and plan the whole journey; we've walked the path hundreds of times and can help you prepare.

We'll help you answer difficult questions

How do we manage 000s of devices in the field?

Is a PoC or MVP required?

When should I introduce at-scale technologies?

?

What new risks might emerge when we transition to scale?

When should I re-engineer various modules or subsystems for mass production?

With the benefit of experience, a coherent strategy can be developed for the entire journey.

Trade off #2 - Make vs Buy

Knowing when to go with off-the-shelf components and when to undertake a bespoke design is driven by the business case.

You'll want to consider things such as:

Security - buying in components can increase the vulnerability of your product. How does your proposed third-party supplier plan to manage vulnerability disclosure? Does this give you less control in future?

Scalability - from development board to custom board to full design for manufacture, when is the right time to transition?

Buy?

Make?

//consult.red

// The scale roadmap

When planning your scale roadmap, what do you need to consider?

2

Considerations

✔ What aspects of the system will require hardening for use in a scale deployment (operating systems for instance)?

✔ Can you do a security vulnerability analysis on bought in components?

✔ How will you do secure, in-field upgrades if required?

✔ What radio and hardwired communications are key to your system?

✔ Will a pre-tested and certified commercially available sub-system module offer a lower cost path to mass production?

✔ What cloud platform will you use? When do I need a device management system?

✔ What bespoke software is required to implement the system?

✔ Does any bespoke hardware represent both the security and scalability required?

✔ What are the appropriate certifications and compliance required of the system and how will this be achieved?

✔ Your scale roadmap – what design and system control do you need to achieve it?

✔ Have you considered using or customising an ODM design to reduce time to market?

✔ Does the scale justify a bespoke approac - is a module approach a compromise?

✔ When will there be obsolescence of any critical components bought?

✔ Direct vs distribution – volume dependent.

In a nutshell

When developing a product destined for high volume, engineering teams will understandably focus on the task at hand, whether that's developing a Lab PoC, an MVP or ramp quantities for a trial. But stepping back to consider the entire path to scale provides an opportunity to maximise reuse, delay capital expenditure, reduce risk and avoid refactoring and re-architecting for scale.

Even early on, products typically need to communicate with the cloud, be upgradable, be secure, have an enclosure and be standards compliant. Proving your scale solution early - while delaying Capex - will reduce your risk and mean that your chances of success are maximised when it's time to scale.

//consult.red

3

What are you trying to prove?

Too often, we've seen PoCs that are too narrow in scope, seeking only to 'prove' a specific innovation. Ultimately, the innovation will only be a small part of the overall product, albeit often vital. Instead, get the most from your PoC.

The Scale Strategy will have identified risks that can fundamentally limit the product's ability to scale. These might include poor connection reliability, weak security, a convoluted installation process or manual upgrades. At low volumes, these risks are manageable, but at scale, they can completely undermine a product's operational feasibility.

Before you make a significant investment in building large numbers, make your PoC work harder to mitigate risks that can be exacerbated by scaling. Be clear about what you're proving and align the PoC scope to the scaling roadmap.

For instance, is it proving the price point, the reliability, the power consumption, the scaleability or another identified risk. Proving scalability will often necessitate expanding the scope of the PoC to include system-level and in-field technologies while still also demonstrating vital innovations.

Aside from mitigating risks, a comprehensive PoC is a powerful tool for reassuring and encouraging investors.

We do a lot of PoC work for our customers, often involving cutting edge technologies. Our approach is always to have clearly identified outcomes that are aligned with the scale roadmap.

Trade off #3
Security: data usage and storage vs functionality

The UK is taking 'decisive action' on IoT security and is taking a staged approach to enshrining 'Secure by Design' standards in law. The UK has also been leading efforts to create international alignment and, as such, has been working with other territories to align standards in the US (NIST) and EU (ETSI). In short, the direction of travel is only going one way.

✓ To implement security in line with the business case, there may be constraints on data use and storage.

✓ Security is sensitive to scale – it needs to be an important element of your scale roadmap.

✓ Don't forget to budget for security – depending on the requirements, 5% - 10% of your product development budget will be required to implement and deploy a secure product.

✓ In the field, around 5% of ongoing costs will be related.

Want more? Check out our in-depth Secure by Design quick guide and checklist

//consult.red

Proof of Concept (PoC)

What are you trying to prove?

Considerations

✔ Try to develop as much of your end-to-end system as is feasible.

✔ Use development boards and off the shelf components to demonstrate the required functionality.

✔ Test wireless connectivity extensively in the field – understand real world coverage and data rate limitations.

✔ Consider trade-offs of where data processing should occur – at the edge, the gateway or in the cloud.

✔ Undertake market analysis of all system components to understand what is available.

✔ Power budgets and power source trade-offs will be linked to the business case and maintenance requirements.

✔ Explore what-ifs of real-world environments – power outages, loss of connection, loss of data.

✔ Be clear what your Po`C is 'proving'. For instance, is it proving the price point, the scalability, power consumption, viability of the software, or functionality of a sensor, serviceability, reliability or security?

✔ Can you test the Proof of Concept in the market or do you need to develop it further?

✔ What evidence is needed for stakeholders - especially funders!

In a nutshell

By expanding the scope, you can use the PoC to prove at-scale technologies such as system-level and in-field technologies. This will help to mitigate risk, reassure stakeholders and even attract investment.

//consult.red

// Minimum Viable Product

Or, should that be Market Viable Product?

Getting to scale is all about risk management, and through your PoC, you've managed the technical risk. But, what about the market risk? You need to apply a commercial lens; front of mind for stakeholders and investors will now be the strength of customer demand and the customer journey's effectiveness.

Unless you have an established market, your new product will need testing with the market that will use it. A Minimum Viable Product (MVP) is an ideal vehicle for doing this. There's no substitute for honest customer feedback and the market insight that it brings.

The MVP is your chance to get into the market swiftly, establish demand, pipe clean the sales and marketing channels and potentially gain a first-mover advantage over your competitors.

Creating a waypoint between the PoC and mass production is a chance to get real-world feedback before committing capital to mass production. Taking a strict and clear view of the minimum viable feature set will enhance an MVP's chances of success and force developers to prioritise those vital features.

Your MVP may lack some of the scale product's features and refinements, but it can still yield insightful customer feedback and valuable data. This data provides a golden opportunity to make improvements and address real customer concerns before going to scale. A successful MVP can be the green light investors are looking for.

We help our customers assess the benefits of an MVP and, if needed, deliver the MVP. In all instances, this has been worthwhile.

Trade off #4
MVP: market testing vs time to market

Understanding the performance of your technology in the field is essential to see your product through your customer's eyes.

Experience of product requirements such as device onboarding, over-the-air updates, failure conditions (loss of connectivity) and other aspects of user experience can guide developing a robust and reliable product in the field.

Test harnesses and processes are essential at the MVP stage and form part of ongoing regression testing necessary for in-field updates.

// consult.red

www.consult.red

Minimum Viable Product

Or, should that be Market Viable Product?

Considerations

✓ The gap between the PoC and desired product can be too large to bridge in one step. MVP can play a vital role in establishing the market and generating real-world feedback.

✓ The minimum viable solution demonstrates the system such that it delivers the basic functionality and outcomes that customers value. It will often form the platform for the final operational system.

✓ Implement the complete communication chain from edge to cloud.

✓ Implement the prototype security model using provisioned keys but not at scale.

✓ Test user interfaces and user experiences with people who will engage with the deployed system.

✓ Further test wireless and other connectivity extensively in the field –understand coverage and data rate limitations.

✓ Reconcile connectivity, communication and cloud costs with the total cost of ownership calculations in the business case.

✓ Identify the technical and market data the business needs and ensure this is collected.

✓ Plan for in-field security management and remedy - anomaly detection, key revocation and remediation.

For over 15 years that we've been developing connected devices, an MVP has always delivered insightful, valuable feedback that has minimised cost and delay in the long run.
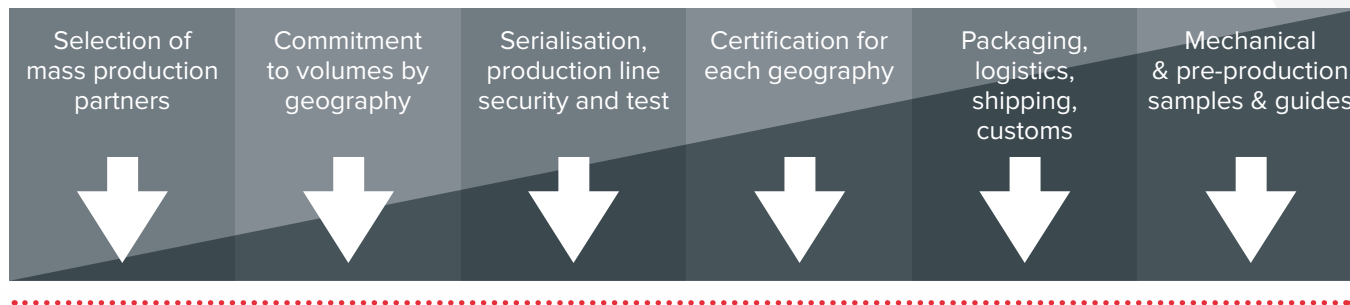
//consult.red

www.consult.red

// Ramping to scale

As you scale up so does cost, and getting it wrong is expensive

Unless you're from a very large organisation with deep pockets, it's likely you'll need significant investment to fund this next stage. That's where experience, along with a solid, robust scale roadmap, PoC and MVP will really pay dividends. New product introduction is an intense stage of the process involving numerous decisions and approvals, such as:

Selection of mass production partners	Commitment to volumes by geography	Serialisation, production line security and test	Certification for each geography	Packaging, logistics, shipping, customs	Mechanical & pre-production samples & guides
⬇	⬇	⬇	⬇	⬇	⬇

Considerations

✔ Factory selection via audit and inspection prior to engagement with mass manufacturer is essential.

✔ Design complexity, advanced component packages, board layers number of sub-assemblies will impact cost of scaling.

✔ Establish technology sweet spot to optimise efficiency of mass manufacture.

✔ Decision on expected enclosure tooling lifetime to cover expected mass volumes. Costs can be high and need to be amortised to determine return on investment.

✔ Check for sole sourcing of components.

✔ Establish reliable and secure alternative sources for all system components.

✔ Establish expected lifetime of all constituents of the system.

✔ Apply design for manufacture philosophy to the various bespoke parts of the system.

✔ Factor in test fixture design and commissioning in advance of pre-production.

✔ Establish criteria for undertaking pre-production build. MVP test parameters acceptable and align with stable software build. Pre-compliance tests acceptable.

✔ Crucial to review, feedback and correct pre-production issues prior to mass production commitment.

✔ Establish procedures for quality assurance checking and continuous improvement processes.

✔ Establish procedures for security monitoring and updating for all bespoke and bought in components of the system.

✔ Establish vulnerability disclosure procedures for the complete system.

✔ Decide where to manufacture bespoke components.

✔ Explore how to deliver security keys at the manufacturing location at scale.

✔ Decide on approach to undertaking regulatory and compliance testing and certifications.

//consult.red

Ramping to scale

Spotlight on security - how much do you trust your manufacturer?

This step is often overlooked - it can compromise your device later - and be very costly to fix!

It is easy to lose track of how secret keys and serialisation data will be handled within the factory.

A leak, whether malicious or entirely accidental, could be disastrous. What due diligence have you done on the factory?

Plan how you'll securely manufacture and deploy your device in the field.

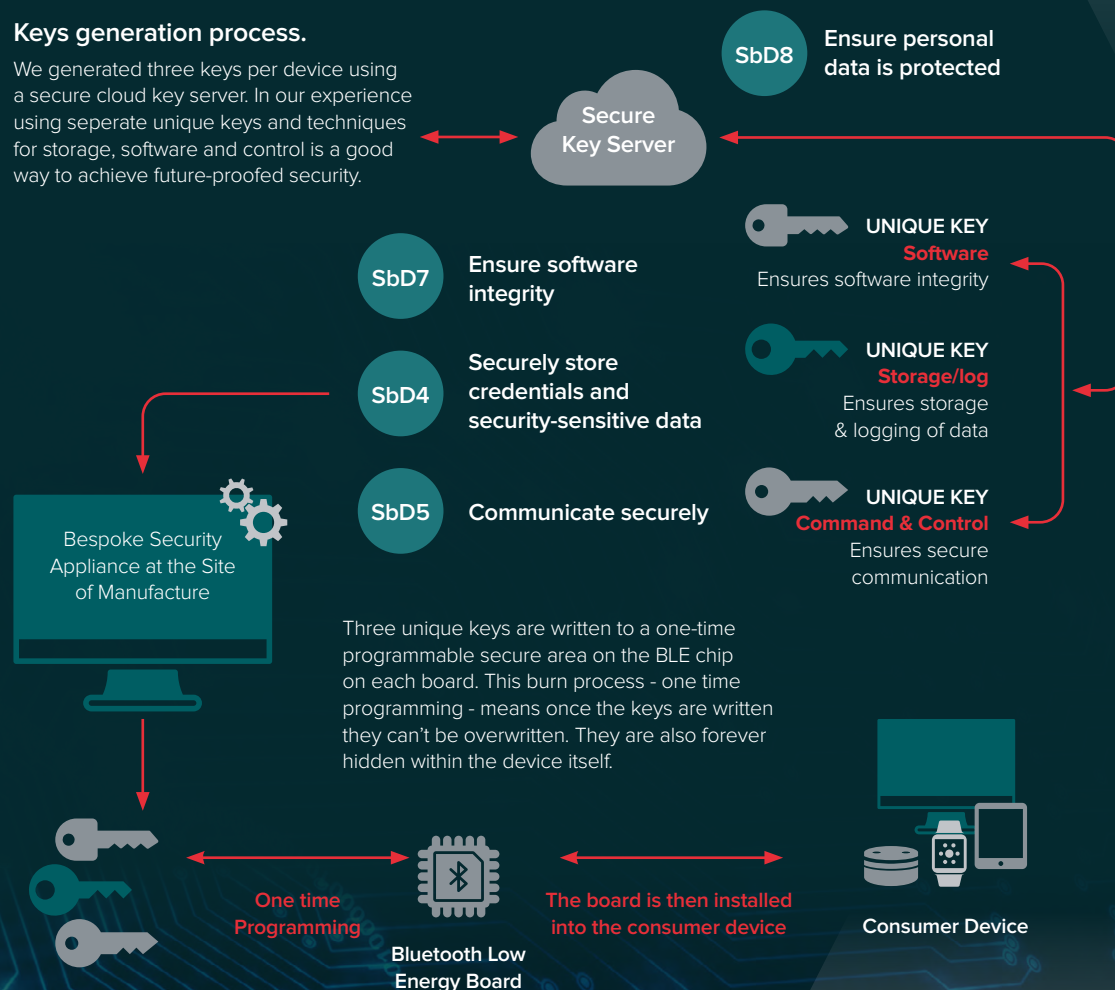**Unique keys** → **Customer Device**

In a nutshell

Experience really counts at this stage - ramping to scale is hard, intense and expensive if it goes wrong.

Example: Delivering secure IoT during manufacture

An example of how we've delivered turn-key, future-proof and secure IoT during manufacture: implementation of a Bluetooth Low Energy board with secure multiple key injection in a smart device.

Keys generation process.

We generated three keys per device using a secure cloud key server. In our experience using seperate unique keys and techniques for storage, software and control is a good way to achieve future-proofed security.

Secure Key Server

SbD8 Ensure personal data is protected

SbD7 Ensure software integrity

SbD4 Securely store credentials and security-sensitive data

SbD5 Communicate securely

UNIQUE KEY Software
Ensures software integrity

UNIQUE KEY Storage/log
Ensures storage & logging of data

UNIQUE KEY Command & Control
Ensures secure communication

Bespoke Security Appliance at the Site of Manufacture

Three unique keys are written to a one-time programmable secure area on the BLE chip on each board. This burn process - one time programming - means once the keys are written they can't be overwritten. They are also forever hidden within the device itself.

One time Programming → **Bluetooth Low Energy Board** ← **The board is then installed into the consumer device** → **Consumer Device**

// Operational system

6

You've launched, but the work is far from over

As mass production becomes part of business-as-usual, the focus will shift to the operational system. Project capitalisation will close, and the spotlight will be on managing operating costs, which typically leads to a rolling programme of cost downs, second sourcing and incremental improvements.

We work with our customers as a trusted partner during the operational stage, helping them as needed to add features, manage security, reduce cost or manage systems. Using a trusted partner to step in when needed or to handle specialist activities helps our customers reduce their operational overhead

Collect insightful data to inform improvements

Tuning in-field data gathering and analysis to answer business improvement questions is an ongoing process. For example:

- How much data is sent per month? Could we switch from GSM to LoRa to reduce cost?
- What latency are we achieving - do we need 5G?

Security & compliance

How will you comply with increasing Secure by Design type regulation? Incoming vulnerability disclosures must be acted upon and a software BOM should be used to pro-actively seek out relevant disclosures.

Upgrades & new features

Innovation and competition move fast. Managed connected devices offer the opportunity for feature upgrades through software updates. It may also be necessary to upgrade security on the devices and systems as well as make disclosures to customers and authorities.

Considerations

✓ Systems are moving from a fire-and-forget approach to a scaled platform that is both live and updateable. A device management system is becoming a must-have.

✓ Security vulnerability policy requires both incoming and outgoing communication with customers and suppliers of system components. This includes monitoring the software community for security intelligence.

✓ What procedures are required to make security and functionality updates? This will include upgrades staggered across the deployment, rollback of updates and in-field system updates.

✓ Technology is constantly evolving, so the system should be reviewed for upcoming technology changes to enable competitors and alter the business case for the current deployment.

In a nutshell

Working as a partner to step in when needed, or to manage specialist activities, we help our clients reduce operational overhead.

// consult.red

// In summary

We've helped to develop hundreds of connected devices and systems – from concept to millions of deployed products - for some of the world's largest brands. We know the journey and can help you manage risk and get to market, faster.

Scaling your product to the hundreds, thousands or even millions brings additional commercial and technical risks that can be easily overlooked during development and early deployment. Getting your IoT product to scale profitably is a multi-stage journey that requires different skills, experience and approaches at each stage.

A robust and agile business case is fundamental. You'll need to understand the Total Cost of Ownership (TCO) of your final product too. You can't plan your ROI if you're not evaluating the operational expenditure that's required to maintain the product at scale over its entire in-field life. Don't forget to budget for security – depending on the requirements, 5% - 10% of your product development budget will be required to implement and deploy a secure product. In the field, around 5% of ongoing costs will be related.

When developing a product destined for high volume, engineering teams will understandably focus on the task at hand, whether that's developing a Lab PoC, an MVP or ramp quantities for a trial. But stepping back to consider the entire path to scale provides an opportunity to maximise reuse, delay capital expenditure, reduce risk and avoid refactoring and re-architecting for scale. Security is sensitive to scale – it needs to be an essential element of your scale roadmap.

Even early on, products typically need to communicate with the cloud, be upgradable, be secure, have an enclosure and be standards compliant. Proving your scale solution early while delaying Capex will reduce your risk and means that when it's time to scale, your chances of success are as high as they can be.

Too often, we've seen PoCs that are too narrow in scope, seeking only to 'prove' a specific innovation. Ultimately, the innovation will only be a small part of the overall product, albeit often vital. By expanding the scope, you can use the PoC to prove at-scale technologies such as system-level and in-field technologies. This will help to mitigate risk and reassure stakeholders and even attract investment.

Getting to scale is all about risk management, and through your PoC, you've managed the technical risk. But, what about the market risk?

You need to apply a commercial lens; front of mind for stakeholders and investors will now be the strength of customer demand and the customer journey's effectiveness. An MVP can deliver insightful and valuable feedback that minimises cost and delay.

Unless you're from a very large organisation with deep pockets, you'll likely need significant investment to ramp up to scale. That's where experience, along with a solid, robust scale roadmap, PoC and MVP will pay dividends.

Once your product is deployed in the market, the spotlight will be on managing operational costs, which typically leads to a rolling programme of cost downs, second sourcing and incremental improvements.

In a nutshell

We've walked the path; we know the pitfalls and the trade-offs. We work with clients at every stage in the journey to:

✔ Accelerate development ✔ Reduce cost and delay ✔ Manage and minimise risk

// consult.red

//consult.red

Connected Devices & Systems

Consult Red is a technology development partner helping clients deliver connected devices and systems, supporting them through the entire product development journey.

We've helped to develop hundreds of connected devices and systems - from concept to millions of deployed products - for some of the world's largest brands. We know the journey and can help you manage risk and get to market faster.

Consult Red has a team of 300 people, based in multiple strategic locations in the UK, USA and Poland.