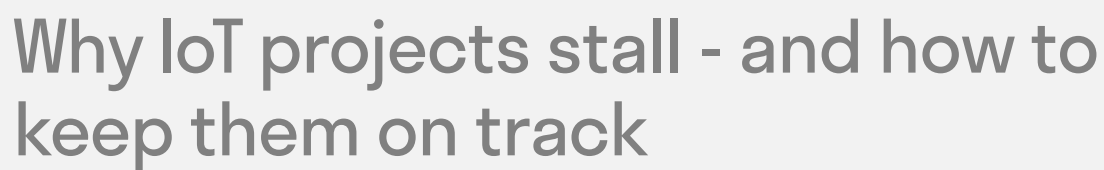


A dark blue horizontal banner with the text "IoT deployment challenges white paper" in white, sans-serif font. A thin red vertical line is on the right side of the banner.

IoT deployment challenges white paper

A light gray rectangular area containing the text "Why IoT projects stall - and how to keep them on track" in a dark gray, sans-serif font. To the right of the text is a small graphic of three colored squares: blue, red, and white.

Why IoT projects stall - and how to keep them on track

A dark gray horizontal banner at the bottom of the page with the text "→ For more information please visit Quectel.com" in white, sans-serif font.

→ For more information please visit [Quectel.com](https://www.quectel.com)

Contents

Introduction	3
Simple starts lead to complex realities	4
Why IoT projects stall	5
The main technical challenges	5
Growing pains	9
The key causes of project delay	10
The hidden supplier problem	11
The end-to-end advantage	12

INTRODUCTION

While IoT adoption continues to accelerate, many projects still fail to progress beyond the pilot stage or achieve the expected return on investment (ROI). It is likely that lack of awareness was an early contributor to project failure and, while much of this has been addressed, failure is now due to scalability issues associated with larger deployments, added technical complexity with more on-device intelligence and the fragmented supplier ecosystem.

Most projects still fail at the pilot or early-deployment stage and this is because enterprises often overlook the complexities involved in a successful IoT project. As volumes have increased, errors, inefficiencies and security vulnerabilities are

amplified, resulting in greater pressure to design, develop and engineer devices that are robust, secure, reliable, scalable and cost effective.

This challenge is compounded by the current generation of IoT devices embedding greater functionality. Put simply, with more being done on the device, there is greater potential for things to go wrong and for disconnects between capabilities and components to occur. Engineers therefore need to ensure that every new function and component can perform optimally. This is being addressed by careful selection of vendors, awareness of the entire supply chain, knowledge of incoming trends in device capability and expertise in secure, compliant product creation.



SIMPLE STARTS LEAD TO COMPLEX REALITIES

For many, the idea of adding connectivity to an existing product or service has been the driver behind IoT. The development process is simplistically viewed as merely selecting a module, an antenna, a SIM and a cloud platform as add-ons to an existing product offering.

The reality is that these components and services only really address about 20% of an entire IoT project with the remaining 80% still needing to be managed after these essentials have been selected. There are numerous hand-offs, performance gaps, integration challenges and misunderstandings between different participants that simplistic approaches overlook.

pre-address these hidden challenges. These providers in effect sell execution capability rather than products and are well-positioned to address the demands of enterprises. Very few enterprises really want to delve into all the minutiae of IoT development, they simply want to get connected products to market quickly and generate revenue and benefits from IoT enablement.



This lack of awareness of the scale and complexity of IoT projects results in additional work and further delays as issues are found and mitigated. Sometimes this means taking a near-complete product back to the drawing board and often-costly re-engineering work is the only way to achieve the initially envisaged outcomes of a project.

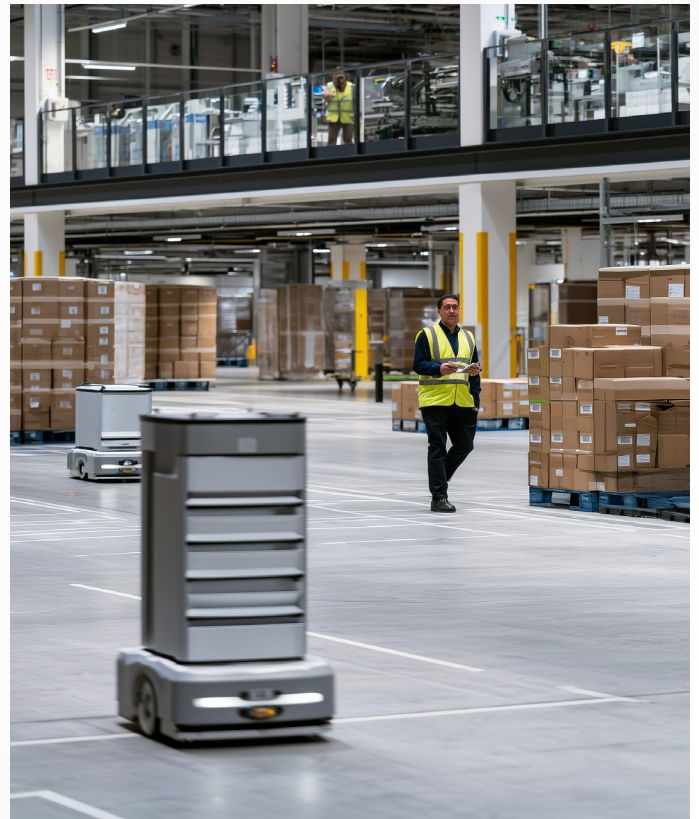
To avoid repeating the excessive failure rate of the last decade, enterprises are increasingly turning to end-to-end providers of IoT solutions that effectively

The technology itself is the barrier that an end-to-end approach abstracts away from the enterprise and places with the IoT services provider. It's therefore time for enterprises to adopt an end-to-end execution strategy that takes account of all the interdependencies and likely changes that will impact IoT devices throughout their deployment lifecycles. Enterprises can't continue with the fragmented approach to specifying discrete components and services that has led to an alarming and unacceptable failure rate across all types of IoT deployments.

WHY IoT PROJECTS STALL

The main reasons IoT projects fail have roots in business, organizational and technical integration challenges. From a business point of view, companies often decide to adopt IoT without a clear use case in mind when they should have already defined a specific business problem for the technology to solve. As understanding increases and experience widens, this is becoming less of an issue and many of the early challenges have been addressed. Even so, inaccurate estimation of the long-term costs of data storage, the expense of continuous and growing international connectivity and the need to maintain large fleets of deployed devices all skew the business case causing project managers to reach for the brakes.

The emergence of unexpected challenges and poorer than expected results often sees projects fail to scale beyond the pilot stage and become lost in a doom loop of never-ending experimentation. This situation is compounded organizationally by the ongoing skills shortage in IoT. There are still fewer expert engineers and developers available to design devices and for many enterprises, there isn't a clear need to build a full-time, permanent IoT development team. For example, an enterprise with a small number of products will only need to enable these once in a generation so the workload doesn't justify maintaining a large internal team.



The technical challenges largely center around integration of products and components from disparate vendors. Each is only responsible for their own piece of the deployment so it's easy to point the finger of blame in other directions or to specify components that need substantial and complex integration work, causing delay and adding costs to projects.

THE MAIN TECHNICAL CHALLENGES

The cellular IoT reality

While many IoT challenges are common across all connected devices, cellular IoT deployments introduce an additional layer of complexity that is often underestimated during the planning phase. Connectivity should not be viewed simply as a procurement decision, but as a long-term strategic choice. Network sunsets, roaming restrictions, evolving eSIM strategies and operator-specific requirements can significantly affect device availability and operational longevity. At the same time, cellular technologies continue to evolve, with transitions from legacy 2G and 3G networks to 4G LTE and LTE-M,

NB-IoT, Cat 1bis, 5G or 5G RedCap and future generations requiring careful roadmap planning. Products expected to remain in service for 10 to 15 years must therefore be designed with technology migration in mind from day one.

Beyond traditional regulatory approvals, cellular devices frequently require operator-specific certifications, introducing additional testing, cost and schedule considerations, particularly for products intended for global deployment. Lifecycle management is equally critical.

Finally, power consumption remains one of the most common causes of deployment disappointment. Battery life estimates developed under laboratory conditions often fail to reflect real-world operation, where network coverage, operator behaviour, firmware implementation and transmission frequency can significantly impact device autonomy.

Successful cellular IoT deployments therefore require a holistic approach that addresses connectivity, certification, lifecycle management and power optimization as core design considerations rather than afterthoughts.

Development delays

Everything from unclear product specification to inability to secure components for testing causes development delays. Lack of experience can hinder development efforts and there is a need for greater uptake of intelligent tools to accelerate the process. Currently, 37% of machine builders have deployed AI-based design failure prediction, with 34% using AI-driven component modelling and design for manufacturability tools, according to IoT Analytics.¹ Generative design remains at an early stage but is gaining traction. The firm says 33% of enterprises have adopted GenAI for CAD generation, and 25% for concept creation.



Certification delays

Certification delays for IoT devices stem from gaps in complex documentation, strict regulatory mandates

such as the EU's Cyber Resilience Act (CRA) or NIST 2 in the US, and testing bottlenecks at accredited laboratories. These friction points lengthen time-to-market and increase compliance costs for hardware vendors. Massive growth in compliance efforts is expected. The global IoT cybersecurity regulatory compliance platform market was valued at US\$3.8 billion in 2025 and is projected to reach US\$31.2 billion by 2034, reports MarketIntelto.²

Redesign impacts

Redesign is the inevitable consequence of not getting a design right the first time. Fixing late-stage hardware or architecture mistakes drives up non-recurring engineering costs, forces full system re-evaluations in which solutions or ways to mitigate issues are found. Redesigns cause delay to overall time-to-market and add significant costs to an IoT project.

Antenna performance issues

Often overlooked until a late stage in the design process, antenna performance issues can cause devices to fail to perform, to use more battery power or to deliver lower than expected connectivity throughput. For latency-sensitive use cases, this is unacceptable so developers should consider what type of antenna, where it should be located and how it should be mounted to the product early in the development phase. Only by doing so can costly adaptations and even redesign be avoided later in the development process.

With worldwide antenna shipments predicted to reach 13 billion units by 2030 according to ABI Research,³ there are enormous choices of antennas available in the marketplace so there's no excuse for not selecting an optimal antenna. In addition, AI-assisted antenna design software tools can help device OEMs virtually test antenna placement and performance based on board size and electronic design. These tools can also assist with component selection and enable direct ordering of antennas and ancillary parts.

¹ <https://iot-analytics.com/ai-in-machine-building-2026-adoption-barriers-use-cases-and-leading-sub-industries/>

² <https://marketintelto.com/report/iot-cybersecurity-regulatory-compliance-platform-market>

³ <https://www.abiresearch.com/press/global-iot-antenna-shipments-to-reach-13-billion-by-2030-despite-lingering-post-pandemic-headwinds>



Supply chain changes

Ensuring available components across silicon, memory and modules as a project scales up and during its lifespan is a critical part of device design. While many of the supply chain challenges highlighted by the pandemic are being mitigated, changes in the supply chain can have significant impacts on devices, requiring alternatives to be designed in and potential repair or replacement work to be undertaken on the installed device fleet.

Developers need to ensure their suppliers understand their needs and will be present for the long-term to support the entire product lifecycle. The IoT device supply chain shouldn't be dependent on a one-time contract for supply of a component that can result in a project failing through unavailability of single component at scale.

Manufacturing problems

IoT and IIoT projects are negatively impacted by manufacturing problems typically caused by complexities and failures in the manufacturing of physical IoT hardware itself. For example, solder joint fatigue or reflow errors can be caused by poor thermal profiling during printed circuit board (PCB) assembly. Other problems are caused by

design that doesn't adequately consider how to smoothly manufacture products. Overlooking ease of manufacture can result in needlessly complex manufacturing with difficult and time-consuming processes that are prone to failure. In addition, manufacturing capacity is sometimes unable to scale up to meet the needs of large IoT deployments.

Designers and developers should therefore focus on simplifying the manufacturability of devices. By selecting fewer components and reducing complexity, the potential to create errors or add steps to manufacturing processes can be controlled and eliminated resulting in higher quality, more robust devices.

Firmware integration failures

This is one of the main killers of IoT project success. While hardware failures are relatively easy to understand and address, firmware failures cause random crashes, rapid battery drains or result in security exposures without necessarily having clear reasons. Project failure is often caused by hardware and firmware teams working separately, with firmware engineers often writing and testing their code using preliminary datasheets or virtual simulators.

Partial updates, incompatible version roll-outs and missing rollback protections regularly cause entire fleets to fail causing huge repair or replace work and significant reputational damage for enterprises.

Firmware should be considered as an integral part of an IoT project with development undertaken alongside the holistic design project. Firmware writers should have access to the latest data and build firmware on finalized, real products, rather than simulators.

Security compliance and updates

Growing regulatory, legal and procurement expectations are shifting IoT cybersecurity from asserted trust toward documented, defensible security assurance. With ABI Research estimating there were 19 billion IoT connections globally in 2025, with that number forecast to grow to 37 billion by 2030 huge growth is projected.⁴ As the number of connections nearly doubles and connected devices proliferate across homes, workplaces, healthcare environments, schools, industrial sites and public sector infrastructure, the expanded IoT device footprint creates risks ranging from compromised data to service disruption, unauthorized surveillance and broader network exposure, the firm says.

Device selection criteria, vendor representations, security certifications, internal reviews, risk sign-offs and lifecycle management policies are increasingly subject to scrutiny from regulators, insurers, auditors and boards. The research firm warns that the absence of documented security assurance could become a central consideration in determining whether an organization exercised reasonable care. Designers and developers therefore need to adopt a lifetime approach of security by design which starts from the beginning of the device concept and runs through manufacture, initialization and eventual retirement with frequent updates and accurate documentation throughout.

OTA management and update failures

IoT, by definition, relies on ubiquitous connections to link the device data to the internet. That same connection is an essential aspect of keeping an IoT device current during what are often very long lifespans. Aftermarket telematics devices are often utilized for many years within vehicle lifespans and sensors and devices such as meters have lives of more than a decade. It's therefore essential that these devices can update over-the-air (OTA). Part of that is ensuring the connectivity is available and resilient enough to complete cost-effective



⁴ <https://www.abiresearch.com/press/the-end-of-trust-me-security-abi-research-cautions-iot-security-is-becoming-a-board-level-governance-risk>

downloads of update packages but designers and developers also need to consider their policies and processes for OTA upgrades.

They need to track and document which devices have had upgrades to firmware, operating systems, specific software and operating functions such as power management or security. They need to be able to know if upgrades are successful so they can be retried if unsuccessful or if they have caused issues so they can be rolled-back. OTA upgrades and other management functions are an essential part of IoT device performance so they need to be considered from the beginning of device design rather than being applied retrospectively.

Certification costs

As regulations tighten across the globe, vendors are building tools for long-term IoT compliance. This extends from redesigning chip architectures and investing in compliance tools that help IoT device manufacturers meet lifecycle obligations. IoT Analytics expects to see growing adoption during 2026 of end-to-end compliance ecosystems that support secure provisioning, certificate management, software bill-of-materials upkeep and vulnerability monitoring across the full device lifecycle.⁵ IoT OEMs in regulated industrial, medical, and automotive markets increasingly combine internal security capabilities with external compliance-as-a-service platforms to meet long-term regulatory obligations without building all tooling in-house.

GROWING PAINS

What is clear from all of these reasons for IoT project failure is that the real challenges occur when a project scales up. It's relatively simple to build a prototype but building 100,000 reliable devices demands that all of these potential pitfalls are carefully addressed as early in the IoT device design and development process as possible. With the

cellular IoT market set for strong growth over the next decade and cellular IoT connectivity projected to reach 5.9 billion connections by 2035 according to Omdia,⁶ large-scale projects are the routine reality. Scale brings complexity and greater consequences for project failure so getting design right first time is an increasing priority.



⁵ <https://iot-analytics.com/iot-semiconductor-predictions/>

⁶ <https://omdia.tech.informa.com/om144827/cellular-iot-market-tracker--1h26-analysis>

THE KEY CAUSES OF PROJECT DELAY

Time, as always is the developer's enemy. The motivation to create an IoT product is to either generate new revenue or create savings through greater efficiency. Often both reasons are the drivers so there's an obvious need and business imperative to develop and take products to market as quickly as possible. Failure to design products that are fast-to-build, selection of a fragmented set of vendors and poor integration of components into the final product all cause delay and the consequences can be substantial.

If you take the example of choosing the wrong antenna, it's clear to see how time and money can be

burnt up. If an antenna is selected but can't perform because it is sited too close to electromechanical interference (EMI) or it consumes too much power or needs to be more compact, an alternative must be selected. However, this isn't a rip-and-replace bolt-on component, it impacts the entire device design. Developers will need to redesign the entire PCB, engage in new radiofrequency testing, get the product re-certified, take in the impacts of production delay such as missing out on factory time and having to wait for capacity to become available. This results in a missed product launch deadline from just this one component. In this scenario, a single poor decision can easily cause six months of delay.

PHASE 1:

STRATEGY AND PLANNING

1. Unclear business objectives
2. Undefined return on investment (ROI)
3. Mispredicting the scale of uptake
4. Getting stuck in the pilot phase
5. Underestimating development time

PHASE 2:

BUDGET AND MANAGEMENT

6. Cost over-runs and poor manufacturability
7. Inaccurate costings for cloud and connectivity
8. Insufficient leadership support
9. Disconnection between IT and OT
10. Internal skills gaps

PHASE 3:

HARDWARE AND TECHNOLOGY

11. Poor hardware design and selection
12. Wrong or delayed antenna specification
13. Power management miscalculation
14. Inadequate environmental and field testing
15. Wrong connectivity choice

PHASE 4:

DATA AND SECURITY

16. Unstructured data and/or inadequate analytics
17. Integration failures
18. Security vulnerabilities and underestimating certification
19. Weak firmware and OTA updates strategy
20. Scalability bottlenecks

THE HIDDEN SUPPLIER PROBLEM

Traditional engineering practice suggested that the best product would be created by assembling the best components for each aspect of a device. Development teams would scour the market to identify optimal components for their projects, carefully balancing performance, availability and cost. That process in itself is long and complex but it doesn't necessarily result in the best possible overall product.

This is because every supplier in the chain is focused on optimizing their part, not the overall product. This means nobody owns the entire product so there is immense scope for vendors to blame neighbouring components or the way in which their product has been implemented. Every hand-off means delays, communication gaps, duplicated testing, ownership disputes and integration issues.

Don't forget the list of ingredients can be long and most IoT companies buy from a module vendor, a SIM provider, a cloud enabler, an original device manufacturer (ODM), a provider of electronics manufacturing services (EMS), an antenna specialist, a design house, a certification lab and a software company. Each of these has interdependencies with each other as detailed above and there is potential for disconnects and failures at each juncture.

The integration burden can rapidly spiral out of control as IoT companies try to align their vendors and fix bugs and issues as they arise. This doesn't stop with completed manufacturing, it can continue for the life of the project. There's an iceberg of complexity lying just beneath the surface of every IoT device.



Table 1: The true cost of integration

Area	Looks simple	Reality
Module	Plug in	Driver development
Antenna	Add antenna	RF tuning
Cellular	Add a module	Coverage, power consumption, certifications
Connectivity	Add SIM	Global roaming
Cloud	Connect	Security architecture
OTA	Firmware update	Device fleet management
Manufacturing	Build boards	Factory programming
Certification	Testing	Multiple regional approvals

THE END-TO-END ADVANTAGE

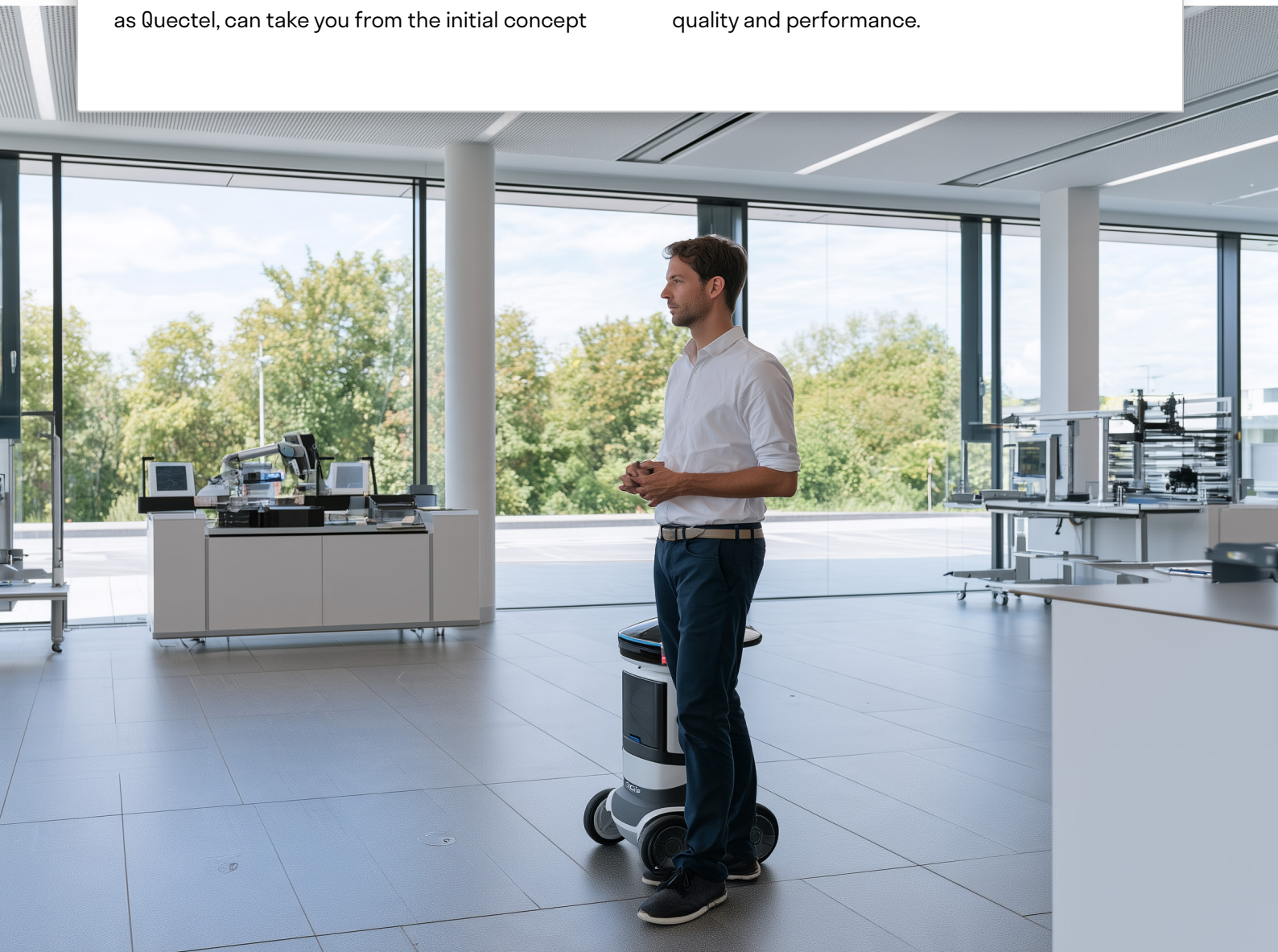
Choosing a smaller number of suppliers or even a single supplier to enable your IoT project from end-to-end eradicates risk, removes complexity, adds speed and saves cost. Simply selecting one end-to-end supplier gives you one supplier to deal with and manage. The intention isn't to stifle innovation but rather to accelerate product introduction at enhanced quality.

The process is streamlined thanks to removing the integration points between suppliers. On top of this, an end-to-end provider will have the deep expertise needed and access to resources to take you through the entire process of product introduction and into operations.

Providers of end-to-end IoT ecosystems, such as Quectel, can take you from the initial concept

and its refinement through reference designs, engineering support and development kits into ODM production. This comprises components including modules, antennas, connectivity and software and is supported by expertise in testing, certification and mass production. The end-to-end ecosystem doesn't end there, it also encompasses lifecycle support, OTA upgrades and device management.

Speed is a competitive advantage in IoT and the simplified, frictionless process that an end-to-end IoT solutions provider can support is the true means to bridge the IoT execution gap. This ensures your IoT product gets to revenue faster, with greater ease while also ensuring product quality and performance.





To find out more about any of our
products or services, please contact:

↗ sales@quectel.com

↗ support@quectel.com



Build a smarter world