Quantum Technologies
Strategic Insight Report

PROTECTING PEOPLE | **ENABLING** AEROSPACE

CAP3200

Published by The Strategic Research and Intelligence Team

James Bell
Innovation Strategy Lead

Lizzy Morgan
Horizon Scanning Principal

Thomas Bristow
Cybersecurity Certification Specialist.

Anirudh Vyas
Future Safety Specialist

To read our past publications visit: caa.co.uk

This publication is available at caa.co.uk/CAP3200

Aviation House, Beehive Ring Road, Crawley, West Sussex RH6 0YR

caa.co.uk

Contents

Introduction

Quantum Technologies are poised to reshape the aerospace sector, offering transformative capabilities across multiple sub-sections of the industry. In August 2025, the UK Civil Aviation Authority (CAA) launched a call for insight into the use of Quantum Technologies within the aerospace sector.

This call aimed to gather perspectives from industry stakeholders, researchers, and technology developers to better understand the current landscape and future trajectory of quantum applications in aerospace. The responses received have been instrumental in shaping this report, which provides a comprehensive overview of the quantum technology market in aerospace.

This report explores both current and emerging use cases for Quantum Technologies across the sector, with a particular focus on current and mid- to long-term potential applications of Quantum Computing, Quantum Sensing, and quantum communication. This report will also aim to explore the rising need for resilience of aviation infrastructure to future attacks from quantum systems. It synthesises the responses received and presents a strategic overview of the quantum landscape, highlighting the implications of these technologies for industry transformation, operational efficiency, and strategic resilience, while also addressing the challenges they present.

As Quantum Technologies continue to evolve, their integration into aerospace systems will require proactive engagement between developers, regulators, and end-users. We hope this report serves as a catalyst for dialogue, encouraging companies developing or considering quantum solutions to engage early with the industry, regulators like the CAA, and identify collaborative opportunities. Our goal is to support safe, responsible innovation and ensure that the UK remains at the forefront of aerospace advancement.

Nonetheless, since the CAA regulates the product rather than the technology, it's challenging to define specific regulatory pathways until Quantum Technologies reach a certain level of maturity. (For example, we may approve a navigation system that uses Quantum Technologies, but not the Quantum Technologies themselves). While we can anticipate user needs, monitor emerging trends, and forecast potential applications, uncertainty remains.

This further highlights the need for early engagement between developers and regulators to address challenges without stifling innovation. We actively encourage those working with Quantum Technologies for aerospace applications to contact the CAA at the earliest opportunity via: Horizon.scanning@caa.co.uk

What to expect in this report

This report explores:

- Current and emerging use cases of Quantum Technologies in aerospace, including Quantum Computing, Quantum Sensing, enhanced navigation, and secure communications.
- Our assessment of the current technology readiness levels across Quantum Technologies, with sensing and communication showing near-term applicability.
- Challenges and risks, including cybersecurity threats, talent retention, and hardware scalability.
- The significance of Post-Quantum Cryptography, Quantum Key Distribution and key industry milestones.
- Regulatory considerations, with emphasis on international collaboration, evolving standards, and the role of the CAA in shaping safe and effective adoption.
- Guidance for technology providers and end-users, encouraging early engagement with regulators and strategic partnerships to ensure safe, scalable, and impactful deployment.

Key Insights

- Quantum Technologies are accelerating across aerospace, with sensing and communication nearing commercial readiness, and computing showing long-term transformative potential.
- Global investment is surging, with over £100 billion in projected revenue by 2035 and the UK ranking second globally in public and private quantum funding.
- Quantum Sensing is the most mature, offering immediate benefits in navigation, timing, and airspace resilience especially in GNSS-denied environments.
- Post-Quantum Cryptography (PQC) is the UK's preferred cybersecurity path, with migration milestones set for 2028–2035, impacting aviation systems and digital infrastructure.
- Quantum Computing trials are underway in airport operations, air traffic management, and aircraft design, with hybrid classical-quantum systems expected by 2035.

What Are Quantum Technologies?

Quantum Technologies are advanced tools and systems built on the principles of quantum mechanics; the science that explains how the tiniest parts of nature, like atoms and particles, behave. These technologies rely on unique phenomena such as superposition and entanglement, which allow quantum systems to operate in ways that classical systems cannot. Although these particles behave in strange and often unpredictable ways, scientists are now learning how to harness their properties to develop powerful new technologies.

Key Areas of Quantum Technology:

There are three main categories, each with significant opportunities for transformation:

Quantum Computing:

These are ultra-powerful computers that use quantum bits (qubits) instead of regular bits. They can solve problems that are too complex for today's computers like simulating molecules for drug development or optimising large systems like transport networks.

Quantum Sensing:

These sensors are incredibly precise. They can detect tiny changes in gravity, magnetic fields, or time and are useful for applications like underground mapping, medical diagnostics, and space exploration.

Quantum Communication:

is a technology that enables the secure transfer of information over distances. There are several applications of the technology. This includes Quantum Key Distribution (QKD) which ensure secure key exchange using quantum principles, while PQC uses advanced mathematical techniques to create encryption methods that would hold steadfast even against a potential quantum attack.

Global Market Outlook

According to market estimates, the three core segments of Quantum Technologies; Quantum Computing, Quantum Communication, and Quantum Sensing could together generate up to £100 billion in global revenue in a decade. Among these, Quantum Computing is expected to dominate, growing from $4 billion in 2024 to as much as $72 billion by 2035.[1]

The United Kingdom is demonstrating strong momentum in this space. A notable increase in new entrants to the UK quantum sector reflects a surge in innovation and commercial interest. Between 2023 and early 2025, the UK ranked second globally in public investment in Quantum Technologies, with a total of $3.5 billion in funding announced.[2] By comparison, Japan led public investment efforts, contributing nearly 75% of the $10 billion total announced globally by early 2025. This dominance came from a single, substantial investment of $7.4 billion made in the first quarter of 2025, far surpassing all other countries.

Meanwhile, the UK, Germany, and the US each committed similar levels of investment between $3.2 and $3.5 billion though they differed in timing and funding strategies. Germany invested heavily in 2023, while the US spread its investment across three years (2023–2025)

Announcement of Public investment in Quantum Technologies between 2023-2025 ($ billion)

Country	2023	2024	Q1-Q2 2025	Total
UK	3.3	0.1	0.1	3.5
Japan			7.4	7.4
Germany	3.2	0.0	0.0	3.2
US	1.0	0.6	1.6	3.2

In 2024, both private and public investors demonstrated increased confidence in the potential of quantum technology (QT) start-ups, investing nearly $2.0 billion globally, a 50 percent increase compared to $1.3 billion in 2023.

While the private sector remained the largest source of funding, contributing approximately 66 percent of total funding, public sector funding, in contrast, rose significantly. This shift reflects a growing sense of urgency among governments to accelerate Quantum Technologies and ensure strategic and national resilience.

[1] McKinsey Digital, "Quantum Technology Monitor", available at quantum-monitor-2025.pdf, June 2025
[2] CAA Analysis of Pitchbook data

The UK's Quantum Technology Strategy

The UK quantum technology market is experiencing rapid growth, underpinned by government prioritisation and targeted strategic investment. The UK Government views Quantum Technologies as strategically critical due to their potential to reshape national security, economic resilience, and technological leadership. Quantum capabilities, particularly in computing, sensing, and secure communications, are expected to unlock new scientific frontiers, protect sensitive infrastructure, and drive innovation across sectors central to the UK's prosperity and global influence. For this reason, the Department for Science, Innovation and Technology (DSIT) has formally designated quantum technology as one of the UK's five priority technologies, underscoring its importance in shaping the nation's future digital infrastructure.

As outlined in the National Quantum Strategy, launched in 2023, the UK is home to at least 160 active quantum tech companies, positioning it as the second-largest quantum ecosystem globally, after the United States. [3] The UK also ranks second worldwide in private investment into Quantum Technologies, and leads Europe in this space, capturing more private equity funding than any other European nation. Between 2012 and 2022, the UK secured approximately 12% of global private-equity investment in Quantum Technologies.

The UK National Quantum Strategy articulates a bold vision: to establish the UK as a leading quantum-enabled economy by 2033, with Quantum Technologies integrated across critical infrastructure and industry. This long-term commitment provides a robust platform for sustained innovation, economic growth, and global leadership.

The UK quantum ecosystem is made up predominantly of SMEs that specialise in distinct domains; hardware, software, algorithms, and enabling technologies. The specialised nature of these areas has accelerated collaboration within the ecosystem, not only across quantum sectors but also with academia, standards bodies, professional associations, allied industries, and end users. This collaborative framework continues to evolve, enhancing the sector's resilience and agility.

In 2022 alone, the UK government funded 139 quantum projects involving 141 organisations through the Innovate UK Commercialising Quantum Challenge, highlighting the scale of public support.[4] This momentum carried into 2025, with DSIT committing £121 million to harness Quantum Technologies to tackle crime, fraud, and money laundering, and to expand real-world applications across the UK.[5]

Additionally, Innovate UK launched a £14 million competition in May 2025 to accelerate development of quantum sensors and positioning, navigation, and timing (PNT) products. These investments signal the UK's continued commitment to building a globally competitive and collaborative quantum ecosystem, equipped to deliver transformative societal and economic impact.

[3] United Kingdom ICT UK Launches National Quantum Strategy
[4] UKRI-03012023-Quantum_projects_brochure2022.pdf
[5] £121 million boost for quantum technology set to tackle fraud, prevent money laundering and drive growth - GOV.UK

Patent Activity

The UK's quantum patent activity reflects a growing innovation ecosystem, especially in Quantum Computing and communications, with over 3,000 patent applications filed between 2000 and 2024, placing the UK seventh globally. Quantum Computing accounts for the largest share with 2,000 applications, followed by quantum communication with over 1,000, and Quantum Sensing with several hundred.[6]

This distribution highlights a strategic focus on computational and communication technologies within the broader quantum landscape, likely because these areas have the greatest potential for cross-industry impact. Quantum Computing and communication technologies are expected to transform sectors such as finance, healthcare, defence, and logistics, offering powerful problem-solving capabilities and ultra-secure data transmission that appeal broadly to both public and private sector priorities.

Quantum Talent

The number of institutions offering quantum-related content continues to grow, driven by supportive government policies and initiatives which aim to expand quantum education across disciplines.

As universities worldwide expand their quantum technology programs, the European Union remains the global leader in producing graduates in quantum-relevant fields. In 2024, the number of universities offering quantum-related programs grew by 8.3%, while those offering master's degrees in Quantum Technologies increased by 10%.[7]

The European Union and the United Kingdom lead in terms of graduate output and density, respectively. The EU has the highest total number of quantum technology graduates, while the UK has the highest density of graduates per capita. India ranks third in total number of graduates, with the EU also maintaining a strong position. The rapid expansion of quantum-related academic qualifications across UK universities is a critical development in building national capability in this emerging field. As Quantum Technologies move from research to real-world application, a skilled workforce will be essential to support innovation, regulation, and deployment.

Leading institutions are responding to this need: the University of Edinburgh offers an MSc in Quantum Informatics, Oxford provides an MSc in Quantum Technologies, and Cambridge's MPhil in Physics includes a strong quantum focus. Cranfield University is also preparing quantum systems engineers through targeted industry-facing programmes. This growing academic infrastructure reflects a strategic effort to ensure the UK is not only advancing quantum science, but also cultivating the talent needed to lead in its practical implementation.[8]

Access to the quantum industry is not limited to university degree pathways. The Quantum Skills Taskforce, a sector-wide coalition comprising representatives from industry, academia, professional societies, national laboratories, and government bodies is actively investing in alternative routes, such as apprenticeships for school leavers, to complement traditional university pathways.

[6] Espacenet and Mckinsey analysis
[7] McKinsey Quantum Technology Monitor, 2024
[8] Training & Skills Hub in Quantum Systems Engineering: The Quantum Enterprise Hub | UKRI

Nonetheless, collaboration between academia and industry in Quantum Technologies is accelerating, driven by a shared understanding that progress in this field depends on both advanced scientific research and viable routes to commercialisation. In the UK, the Quantum Technology Hubs, funded by UK Research and Innovation (UKRI), exemplify this partnership by bringing together universities and industry to co-develop technologies in areas such as Quantum Sensing, computing, imaging, and communications. One example is the National Quantum Computing Centre (NQCC), which opened applications for the second cohort of its Doctoral Studentship Scheme. This initiative will support 30 PhD students across five annual cohorts, with research projects jointly developed by the NQCC and UK university partners.[9]

The growing number of quantum-related job postings in the UK reflects accelerating demand for talent across this emerging sector. In July 2025 alone, over 200 quantum technology-related roles were listed on LinkedIn and more than 300 on Indeed spanning consulting, academia, engineering, and software development.[10] This highlights the growing demand for quantum expertise across the broader economy and reinforces the importance of aligning education and training with industry needs.

International efforts

The European Commission has also proposed a Quantum Strategy to establish Europe as a global leader in Quantum Technologies by 2030. Developed in collaboration with EU Member States and the European quantum community, the strategy focuses on research and development particularly applications in key public and industrial sectors, quantum infrastructure, talent attraction and retention, and the development of a Quantum Technology Roadmap in Space in partnership with the European Space Agency.

As part of this initiative, the EU aims to establish common technical standards and certification frameworks to ensure security and cross-border compatibility across Member States.

This standardisation effort aims to address a major challenge in today's quantum technology landscape, where companies must currently navigate differing protocols across European markets. A proposal for a European Quantum Act is expected in 2026 to support the implementation of the strategy.[11]

In the United States, the 2018 National Quantum Initiative Act aims to accelerate quantum research and development to advance both economic growth and national security. Many other countries including Canada, Germany, and Switzerland have launched bold national quantum strategies to secure their positions in the rapidly emerging quantum economy.

Relevance to Aerospace

Quantum Technologies have the potential to transform the aviation industry across a wide range of operational and strategic areas. They present a wide range of promising applications including ultra-precise inertial navigation systems that are independent of satellite positioning; enhanced materials modelling for developing lighter and more fuel-efficient aircraft; and improved methods for aircraft monitoring. Quantum Computing could be used to optimise complex airline logistics; streamline air traffic management;

[9] NQCC Doctoral Studentship Scheme 2026: Call for EOI - NQCC
[10] LinkedIn and Indeed.com search 21 June 2025
[11] Quantum Europe Strategy: Quantum Europe in a Changing World | European Commission

and improve predictive maintenance. These innovations promise to improve airline efficiency, elevate the passenger experience, drive improvements for Original Equipment Manufacturers (OEMs), and enhance the performance of air traffic management systems.

As the technology matures, quantum solutions are expected to become integral to aviation's digital transformation, boosting resilience, operational efficiency, and competitiveness across the value chain. This rising potential is driving increased collaboration between quantum researchers and aerospace stakeholders, with several aviation companies already engaging in pilot projects and strategic research partnerships to explore these applications.

Currently, Quantum Technologies are at varying Technology Readiness Levels (TRLs), reflecting a varying level of maturity from foundational research to near-commercial solutions, with Quantum Computing at earlier stages of development.

Nonetheless, investment, interest, and innovation in these fields are accelerating rapidly. Governments, industry leaders, and venture capital firms are increasingly backing quantum initiatives, recognising their potential to reshape sectors such as aerospace.

Regulatory Activity and Standards

In the UK, organisations have taken proactive steps to shape both domestic and global standards relating to Quantum Technologies. For example, the CAA is actively involved in the UK Quantum Regulators Forum, its Cybersecurity Working Group, and the Department for Transport's (DfT) Quantum User Group for Transport, contributing to cross-sector coordination and regulatory preparedness. Meanwhile, the British Standards Institution (BSI) serves as a secretariat in the IEC/ISO JTC 3 , a technical committee tasked with developing international standards for Quantum Computing, communications, and sensing. In parallel the National Metrology Institute (NMI) is driving standardisation efforts through the NMI-Q initiative, and the Organisation for Economic Co-operation and Development (OECD) is exploring principles for responsible development of Quantum Technologies.

These platforms support coordination among UK regulators as they prepare for the impact of Quantum Technologies in their respective sectors. They also serve as mechanisms for building shared knowledge, fostering collaboration, and promoting the exchange of best practices.

But it is important to acknowledge that aviation operates within a global regulatory ecosystem that is based on common rules and trust. Most aircraft operating in UK airspace are certified by authorities such as the FAA (US) or EASA (EU), and any new technologies must be recognised as a viable undertaking by these national regulators to ensure continued alignment of safety.

As such, unilateral progress in the UK, while valuable, must be accompanied by international collaboration with other National Aviation Authorities (NAAs) and the International Civil Aviation Organization (ICAO).

Quantum Technologies, opportunities, risks and regulatory implications for UK aviation.

Quantum Computing

Quantum Computing promises performance gains on problems like materials discovery, complex optimisation and simulation, with early access expected via cloud services that pair classical and quantum resources. For aviation, the near-term relevance is in optimisation of flight scheduling, cargo loading and airport operations, plus long-horizon R&D in materials and propulsion. This is done through a method of computing known as quantum annealing. The technology currently remains at low-to-mid TRLs, and practical advantage will be narrow and use-case specific in the next five to ten years.

For the CAA, the regulatory lens needs to focus on three areas: responsible use of international cloud infrastructure and data transfer controls; assurance of safety cases when quantum is embedded in decision support or autonomy pipelines; and preparation for cybersecurity externalities as capabilities mature. Quantum annealing, an optimisation-oriented approach are already piloted in traffic management and Advanced Air Mobility (AAM) planning, will likely be where UK operators first experiment. The CAA can potentially enable safe trials through sandboxes and guidance on evidence standards, while monitoring talent, market concentration and claims of “quantum advantage” with a healthy scepticism.

Quantum Sensing

Quantum Sensing is the most technically mature of the set. It offers step-changes in precision for timing, navigation and detection, and is directly relevant to aviation resilience. Optical and microwave quantum clocks, along with quantum accelerometers and gyroscopes, could provide alternative PNT in Global Navigation Satellite System (GNSS)-denied or degraded environments, which speaks to known risks from jamming and spoofing, and aligns with emerging UK and EU trials in airspace monitoring and counter-UAS.

For the CAA, the strategic opportunity is to shape requirements for integrating quantum sensors into aircraft and ground systems, including certification paths, performance verification and environmental constraints like temperature control. Early engagement with UK hubs and industry pilots will help define evidence thresholds for promised gains in approach and landing accuracy, situational awareness and autonomy support. The CAA can accelerate safe adoption by clarifying test protocols and interoperability expectations with existing PNT and surveillance infrastructure.

Quantum Communications

Quantum Communications, primarily Quantum Key Distribution over fibre or satellite, is progressing through UK testbeds and European space initiatives, and is being explored for aerodrome and air-to-ground links. Importantly, the UK NCSC does not currently endorse QKD for high-assurance government use without additional authentication, it recommends prioritising Post-Quantum Cryptography for practicality and interoperability, which directly affects procurement choices and messaging to industry.

For the CAA, the priority is to provide clear guidance that positions QKD as a potential complement, not a substitute, to PQC in aviation communications, and to ensure any trials include robust authentication, key management and systems assurance. Participation in satellite optical ground station trials and relevant standards efforts will let the CAA influence realistic deployment models, while avoiding the pitfall of mandating specialist hardware where software-based PQC can deliver the required assurance sooner and at lower cost.

Post-quantum cryptography

PQC is the actionable cybersecurity response for the next decade, it replaces vulnerable public-key algorithms that will be broken by future quantum computers, and it addresses the harvest-now-decrypt-later risk that is already present. NIST finalised initial PQC standards in 2024, and the UK NCSC has issued migration milestones for large organisations to define goals and discovery by 2028, early migrations by 2031, and complete migrations by 2035, this timetable is directly relevant to aviation corporate systems and to any move toward digital trust frameworks in safety systems.

For the CAA, the near-term action is twofold: begin exploring methods to adopt PQC within our own estates to set the example and credibility; while also signalling to the sector that PQC-readiness will become expected in regulated digital services (including EFB data links, airport security systems and aircraft ground connectivity). Recommendations on the development of adoption should emphasise crypto-agility, inventory of cryptographic dependencies, quantum-grade entropy sources, and staged migration plans aligned to the NCSC dates, while coordinating internationally to avoid fragmentation in standards and cross-border operations.

Guidance for quantum technology providers and end-users in Aerospace:

Technology Providers:

- **Identify Core Technologies**
  Determine which quantum technology (e.g., computing, sensing, communication) is best positioned to address unmet needs in aerospace operations.
- **Ensure Safety, Privacy, and Compliance**
  Technologies must meet the highest safety standards while also complying with regulations around privacy, data protection, cybersecurity, and consumer protection.
- **Clarify Contractual and Product Liabilities**
  Quantum Technologies may introduce complexities in contracting practices. Consider: how to measure performance accurately (e.g., due to the speed and unpredictability of Quantum Computing). How to draft liability provisions, especially for data loss or errors that are difficult to foresee or quantify.
- **Leverage National Expertise**
  Collaborate with UK academic hubs and national quantum test beds to validate technologies and accelerate development.
- **Engage early with the CAA**
  Involve the CAA at the earliest opportunity if developing aerospace specific products to ensure alignment with regulatory frameworks and safety protocols.
- **Consider evolving international standards**
  Quantum Communications technology providers must consider evolving international standards and take NCSC guidance into account, as required under Network and Information Systems (NIS) Regulations and the UK GDPR.

End Users:

- **Assess potential opportunities and develop future resilience**
  Develop a plan or framework to understand current vulnerabilities and future resilience needs. This will help identify where Quantum Technologies offer practical advantages over classical systems and how they can be integrated into digital transformation programmes.
- **Identify and partner with suitable vendors**
  Engage with technology providers who can offer intellectual property, specialised skills, and implementation support. Strategic partnerships will accelerate readiness and ensure successful deployment of quantum solutions.
- **Offer training to in-house teams**
  Before the full-scale rollout of Quantum Technologies, organisations should consider offering targeted training to in-house teams to build foundational understanding and operational readiness.
- **Assess talent requirements**
  Organisations should identify gaps in quantum expertise and plan for recruitment or partnerships with academic institutions and industry specialists. Building internal capability early will help ensure smoother adoption, reduce reliance on external consultants, and foster innovation from within.

Next Steps

The CAA will continue to engage with industry through a series of workshops planned for 2026, aimed at shaping its thinking on a potential Quantum Strategy. In addition, we actively encourage innovators working on Quantum Technologies to get in contact through our CAA Innovation Advisory Services which provide a valuable platform for testing and exploring emerging technologies in a controlled environment, helping to inform regulatory approaches and support safe, responsible innovation in the aerospace sector.

Further Reading

- > Exploring Quantum use cases for the aerospace industry
- > National Quantum Strategy
- > Quantum Communications: new potential for the future of communications
- > Quantum-Secure Hybrid Communication for Aviation Infrastructure
- > Quantum Technologies and Quantum Computing in life sciences: transformative potential and legal challenges
- > Quantum Technologies in Defence and Security
- > US National Quantum initiative
- > Survey of Quantum Technologies in Aerospace
- > What Happens When 'If' Turns to 'When' in Quantum Computing?

Annex: Quantum Technologies Deep Dive

1. Quantum Computing

Current Status: TRL 3-4

Quantum Computing harnesses fundamental principles of quantum mechanics such as superposition, interference, entanglement, quantum logic gates, and measurement to process information in ways that can significantly outperform classical computers for certain complex tasks. Unlike classical computers, which rely on bits that represent either 0 or 1, quantum computers use qubits, which can exist in multiple states simultaneously. These systems operate at the scale of atoms, electrons, and photons, encoding and manipulating information by precisely controlling quantum states. This enables quantum computers to solve problems are a faster rate than classical computers.

One of its most promising applications is in molecular modelling and simulation, which can be used to accelerate the discovery of new materials, pharmaceuticals and increase efficiencies by up to 30 percent.[12]

Such innovations are particularly valuable in the development of quantum batteries, which could transform energy production and catalysis in fuel cell operations. By drastically reducing charging times, quantum batteries may enable fast-charging electric vertical take-off and landing aircraft (eVTOL) aircraft, as well as advanced energy storage systems capable of managing bursts of energy from renewable sources.[13] In parallel, Quantum Computing is being actively explored to enhance lithium-ion battery technology, potentially leading to safer and more stable batteries that are less prone to thermal runaway and explosion.

Beyond energy applications, Quantum Computing offers powerful tools for optimising complex planning and scheduling tasks. This makes it especially useful in logistics, supply chain management, and resource allocation particularly in sectors such as aviation and automotive. It could improve design, manufacturing, and simulation processes, reduce aviation-related carbon emissions, and streamline operations. For example, quantum algorithms could optimise the loading of air cargo containers, a process that is currently labour-intensive and costly.[14] It also shows potential for improving network optimisation, including high-scale traffic routing, flight scheduling, and the efficient handling of high-dimensional data in areas like satellite communication and energy distribution.

More broadly, Quantum Computing enables the modelling of highly complex systems that are computationally infeasible for classical machines. This includes simulating economic dynamics, social patterns, and the formation of space systems. Each of these domains involves countless interacting variables that require advanced computational power to simulate or optimise effectively.

[12] BCG Report: What Happens When 'If' Turns to 'When' in Quantum Computing. Projects Quantum Computing could represent an efficiency increase of up to 30% for top pharma company with an R&D budget in the $10 billion range.
[13] NASA Technical Memorandum 0000
[14] Feasibility study on quantum optimisation of aircraft container loading | Unisys, University of Newcastle and NQCC

The ability to solve optimisation problems is particularly important in sectors such as logistics, transport, and warehousing, where determining the most efficient routing, scheduling, and resource allocation can yield substantial cost savings and operational improvements. In the financial sector, quantum algorithms are also expected to transform asset pricing, risk assessment, and portfolio optimisation by delivering models that are both more accurate and computationally efficient than those enabled by classical computing.[15]

It is believed that early-stage quantum computers will be deployed via cloud computing infrastructures, allowing users to access quantum capabilities remotely while leveraging classical computing resources for hybrid processing. Initially, these applications are unlikely to involve the processing of personal data. However, there is ongoing research by the Information Commissioner's Office (ICO) to explore potential use cases where personal data may be relevant. In the short-term accessing quantum computers is likely to involve at least some access to international infrastructure, but as with current cloud services, any transfer of personal information will need to comply with international transfer requirements.

Government initiatives

Quantum Computing continues to gain momentum, driven by government initiatives, public-private sector collaborations, and active research communities. In the UK, the government's Industrial Strategy announced earlier this year includes a £670 million investment to accelerate the development of Quantum Computing.[16] This includes a 10-year funding commitment for the National Quantum Computing Centre (NQCC), which has helped shift focus toward practical applications of Quantum Computing.

This effort is further supported by the Digital Catapult Quantum Technology Programme, an initiative designed to raise awareness, educate end users, and foster industry partnerships to drive future adoption and commercialisation of Quantum Computing. The programme forms part of a broader initiative under the Innovate UK Industrial Strategy Challenge Fund (ISCF), which aims to integrate a quantum computer within a classical data centre, enabling exploration of real-world access and applications for Quantum Computing in enterprise environments.[17]

While much of the progress to date has been concentrated in sectors such as drug discovery and financial services, there is growing interest within the aviation industry. Government-backed sandboxes are beginning to explore practical use cases in the sector, such as leveraging Quantum Computing to reduce carbon emissions and optimise loading areas for air cargo.

Looking ahead, the UK aims to build quantum computers by 2035 that outperform today's most powerful supercomputers. These systems could drive breakthroughs in areas such as medicine development, financial services, and clean energy, with potential applications of these advancements likely to extend into the aviation sector over time.

Despite these ambitions, Quantum Computing remains in its early stages. Adoption is still limited, with only a few isolated examples of companies using it for complex optimisation problems. Industry analysts expect Quantum Computing to remain relevant primarily for niche use cases, at least in the near-term, but practical, scalable quantum computers have yet to be achieved.

[15] Dylan Herman et al., A Survey of Quantum Computing for Finance, Arxiv, 2022
[16] UK government announces £670 m for Quantum Computing - NQCC
[17] Quantum Technology Programme - Digital Catapult | Digital Catapult

Nonetheless, major corporations, including IBM, Ernst & Young, Google, and Deloitte are actively exploring and promoting Quantum Computing. These early efforts are often driven by a desire to stay ahead of the curve, particularly within R&D departments. In the aviation sector, such initiatives may lead to Quantum Computing solutions being procured to optimise operations in the coming years.

The UK's broader Quantum Computing ecosystem, driven by initiatives such as the National Quantum Technology Hubs and academic institutions is increasingly exploring use cases in sectors like transport and infrastructure. However, other aviation-specific Quantum Computing projects remain relatively limited in the UK. Globally, the aviation-focused Quantum Computing ecosystem is growing, with most developments led by private sector collaborations. Early-stage pilots and engagement have generally been welcomed by airlines and airports (where many of the benefits are concentrated) as opportunities to streamline operations and deliver cost savings to passengers. These initiatives include experiments by airlines and airports, either independently or in collaboration with academia, aimed at addressing challenges like flight scheduling, fuel optimisation, and traffic flow management in or around airports.

Quantum Computing in Aerospace

Stakeholder	Use Case Applications	Stage	Benefits
Airports	> Traffic flow optimisation (ground & airside) > Baggage routing > Energy use prediction > Scheduling > Gate Assignment	Early Pilot	Improved operational efficiency, reduced delays, lower emissions
Airlines	> Flight scheduling and route optimisation > Fuelling > Repairs and maintenance > Short-term allocation of aircraft and crew rostering	Early Pilot	Reduced delays, efficient resource use, improved scheduling efficiency
Drone Operators	> Manage 3D airspace and swarm traffic in real-time	Early Pilot	Drone traffic management in complex urban environments
Air Traffic Management	> Dynamic routing and conflict elimination for congested airspace > Flight Trajectories	Research	Improved capacity, smoother flows
OEMs/Aircraft Management	> New Materials/ components > Aerodynamics > Flight simulations > Fluid Dynamics > Process optimisation > Flight Decks	Research	Improved operational efficiency and predictability

Potential timeline for development of Quantum Computing in Aerospace:

0-5 years	5-10 years	10-15 + years
> Research and pilot of quantum computers. > Industry and academia partnerships to test use cases > Remote versions of quantum computers available via the cloud and UK Hubs for research purposes and industry testing. > Regulatory engagement	> Mid scale computers may see quantum advantage for some applications. e.g improving machine learning > Demonstration of quantum advantage (1000 qubits or more) for aerospace applications > Improved, accessible and stabilised hardware available	> Classical and Quantum Computing systems operate together in hybrid aviation infrastructures. > Quantum computers capable of demonstrating high impact in sectors such as aerospace, healthcare and finance > Privacy-Enhancing Technologies(PETs) and quantum databases

Illustration of what Quantum Computing could look like in Aerospace

Aerospace 2035...

In the 2030's, aerospace had entered a new era, one powered by Quantum Computing.

At the UK Quantum Aerospace Command (UKQAC), Anil, a lead quantum architect, oversees a fleet of aircraft managed by a quantum computer named QORUS (Quantum Optimisation and Real-time Uncertainty Solver). Unlike classical systems, QORUS doesn't just process data, it explores millions of probabilistic flight paths simultaneously, allocating them into the most optimal route in real time.

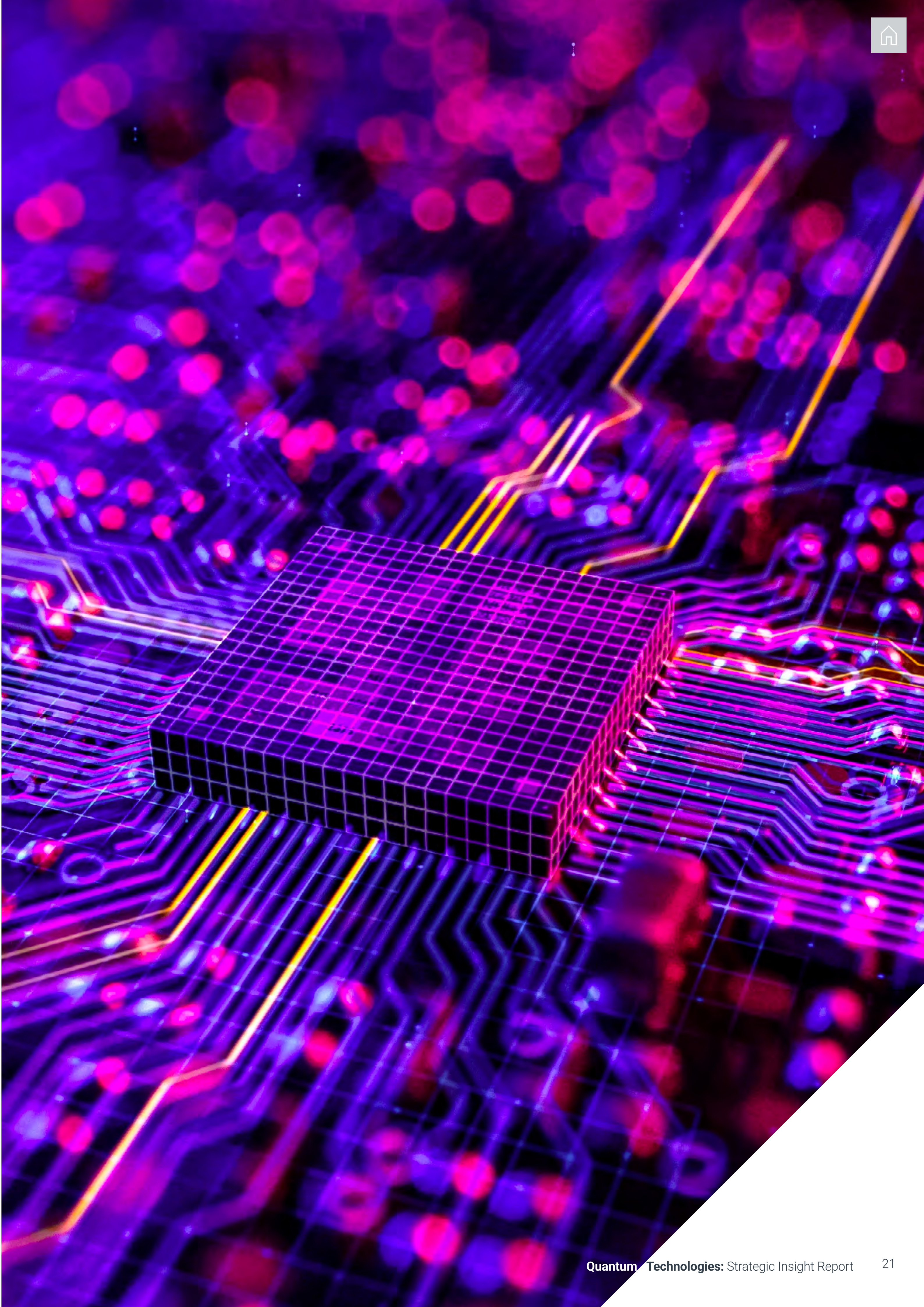
One Sunday, Anil was monitoring Flight QX-0, a next-gen supersonic jet flying from New York to London. The aircraft's onboard quantum processor was entangled with QORUS, allowing it to receive instantaneous updates on weather, air traffic, and even geopolitical airspace changes.

Mid-flight, severe turbulence threatened to disrupt air routes. Classical systems would take minutes to reroute flights. QORUS, using Quantum Computing, recalculated the safest and most fuel-efficient detour in microseconds, factoring in turbulence, wind patterns, aircraft performance, and pilot competence.

Meanwhile, quantum machine learning models onboard QX-0 predicted engine wear patterns and adjusted thrust dynamically to enhance performance. The aircraft wasn't just flying, it was learning, adapting, and evolving mid-air.

Back at UKQAC, Anil watched as QORUS simulated thousands of future scenarios, preparing for contingencies that hadn't even occurred yet.

As QX-0 landed in London Heathrow, passengers were unaware of the quantum optimisation patterns that had unfolded above the cloud. But Anil knew: the skies had changed forever; Quantum Computing had turned aerospace to a predictive ecosystem.



Quantum Computing Challenges

One of the main challenges of Quantum Computing is the high cost of hardware. This is largely due to the complexity of materials, intricate fabrication processes, and the need for extreme cooling to keep systems operational. Even companies that have developed their own infrastructure often offer access to research communities, who then face additional hurdles such as high pricing options and reliance on commercial cloud platforms for data management and storage. This poses a significant issue for government and defence organisations, who are unwilling to store sensitive data in the cloud due to security concerns.

In the UK, UKRI is collaborating with industry and academia to develop quantum hardware and establish a national testbed for UK users. Additionally, some organisations are exploring the potential of hybrid private–government cloud infrastructures to support secure and scalable Quantum Computing environments.

Despite growing interest in Quantum Computing, scepticism remains about its real-world potential. The U.S. Defense Advanced Research Projects Agency (DARPA) is addressing this through its Quantum Benchmarking Initiative.[18] The goal is to determine whether quantum computers can truly outperform classical systems.

In essence, the initiative asks: *If a fully functional quantum computer appeared today, what could it do that a conventional computer cannot?*

The initiative aims to assess whether any quantum approach could become operational at a utility scale by 2033 and disprove quantum computers. Eighteen companies are participating, each working to demonstrate that Quantum Computing can deliver transformative capabilities.

While the number of quantum-related jobs is steadily growing, the industry faces a significant challenge in retaining talent, particularly within academia. Researchers often train for several years in academic settings before transitioning to the private sector, drawn by more competitive salaries and resources. This talent migration can create an imbalance, with the private sector advancing rapidly while academic and public institutions struggle to keep pace. To ensure sustained collaboration and innovation, both sectors must develop sustainable strategies for attracting and retaining talent, fostering a balanced and resilient quantum ecosystem.

The use cases for Quantum Computing are multifaceted in aviation. However, alongside these benefits, there are significant risks, particularly in cybersecurity. One of the most pressing concerns is that quantum computers could eventually break current public key encryption schemes, which underpin much of aviation's global infrastructure.[19]

Beyond cybersecurity, Quantum Computing technologies could have far-reaching operational impacts. They also raise complex regulatory challenges. A key issue is that regulatory bodies typically oversee the products of technology, not the technology itself. This makes it difficult to anticipate how Quantum Computing will be governed, especially as its capabilities evolve over time.

[18] QBI: Quantum Benchmarking Initiative | DARPA

[19] While the corporate end of aviation is encrypted; however, a lot of safety critical aviation systems are not encrypted. For example, communication between an aircraft and an ATC is still unencrypted

Quantum Annealing

Quantum annealing is a form of Quantum Computing that use quantum mechanical principles such as superposition and quantum tunnelling to solve complex optimisation problems. It works by mapping a problem onto a quantum system where each possible solution corresponds to a configuration of qubits. The system then explores these configurations to find the one with the lowest energy state, which represents the optimal solution.

Unlike classical algorithms that evaluate solutions sequentially, quantum annealing evaluates many possibilities simultaneously, making it particularly effective for problems with vast solution outcomes. This makes it ideal for tasks like route optimisation, scheduling, and resource allocation in aerospace and other industries.

In a typical scenario, a quantum processor identifies the most efficient solution by settling into the lowest point in the energy landscape. These optimal configurations of qubits are then translated into usable values.

Once the solution is found, it is transmitted back to the user's program over the network, enabling real-time decision-making based on quantum-optimised outcomes. This approach allows for faster, more accurate solutions to problems that would be computationally intensive or impractical for classical systems.

In the UK quantum annealing is one of a few currently marketable forms of Quantum Computing. It is seen as a practical stepping stone towards achieving broader Quantum Computing goals and this is already being acknowledged and pivoted by several government departments looking to utilise Quantum Computing properties including quantum annealing to optimise their performance.[20]

In aerospace, quantum annealing is especially useful for solving complex optimisation problems related to airports, airlines, ground handling, and AAM. This includes optimising air traffic management to evaluate how new types of air vehicles such as drones, eVTOLs, and supersonic aircraft will operate within shared airspace. Quantum annealers already have tested use cases in aviation, particularly in airport operations and airline logistics. Similar inspiring applications are emerging in other sectors, such as emergency response services.

However, the UK quantum annealing market remains largely monopolistic, with a single dominant provider currently offering quantum annealers tailored for optimisation problems. But a growing number of companies are developing quantum software solutions that incorporate optimisation algorithms compatible with annealing-based architectures, broadening accessibility and potential applications.

Real-world use cases in aviation are already emerging fast. For instance, OneSky announced completion of its first phase of a Quantum Computing Pilot Program focused on Urban Air Mobility (UAM) optimisation. The project utilised quantum annealing techniques to demonstrate how real-time, three-dimensional air traffic control systems could be optimised to safely manage future skies populated by thousands of Urban Air Mobility vehicles.[21]

Despite limited competition, quantum annealing remains the most accessible solution for many organisations looking to optimise their operations.

[20] North Wales Police piloted the use of quantum annealing for emergency operations

[21] OneSky Completes Phase 1 of Quantum Computing Pilot Program for Urban Air Mobility Optimization

2. Quantum Sensing

Current Status: TRL 6-7

Quantum sensors are advanced devices that detect extremely subtle physical changes such as variations in magnetic fields, gravity, and temperature with a level of precision far beyond that of traditional sensors.

They are already being used in radar systems, high-resolution microscopy, and magnetometry, and have profound advantages in industries like pharmaceuticals and healthcare by providing better medical diagnostics.

Quantum Sensing holds promise across a wide range of other fields. It could support automated and autonomous aircraft, refine navigation systems, and strengthen military and law enforcement surveillance. In these areas, the ability to detect minute changes with exceptional sensitivity could offer significant strategic and technological advantages.

Quantum sensors come in two generations. The first generation, which includes technologies like microwave atomic clocks and superconducting quantum interference devices (SQUIDs), has been in use for decades. The second-generation featuring innovations such as gravity sensors, quantum accelerometers, gyroscopes and nitrogen-vacancy (NV) sensors) is now emerging and opening new possibilities.

Second-generation Quantum Sensing is being explored across at least 8 distinct application areas, each varying in terms of technological maturity and market potential. The most competitive applications will be those where no alternative technology exists, or where quantum sensors offer superior sensitivity at a comparable or lower cost than existing solutions.

Key emerging applications include:

> Bioimaging, such as advanced heart or body imaging

> Environmental monitoring, including predicting and monitoring volcanic eruptions, sea levels, or tracking CO_2 emissions

> Infrastructure monitoring, for assessing building stability or detecting leaks

> Geographical surveying, to help locate minerals or oils

> Navigation, especially in environments where GNSS is unreliable, like inside buildings or underground

> Detection of small moving objects in congested areas i.e drones

> Airspace monitoring

> Detection of hydrogen leaks

Quantum Sensing technologies particularly timing applications like optical clocks, are highly relevant to aerospace due to their ability to deliver extremely precise time measurements. First-generation quantum clocks are already used to coordinate high-speed online communications and support navigation systems like GNSS.

However, integrating next-generation optical clocks into navigation systems could offer a faster, more accurate, and more resilient alternative to GNSS, especially in environments vulnerable to jamming or spoofing by malicious actors. This is particularly important in aviation, where GNSS reliability is critical, and interference can pose serious risks.

Quantum sensors are seen as the next era and key use case to address jamming and spoofing in commercial aviation. Our global navigation satellite systems (GNSS) including Galileo and the European geostationary navigation overlay service (EGNOS), are usually considered as suitable technologies for providing PNT information, but they can be vulnerable to local (e.g., interference, spoofing, jamming) or global outages.

There is now growing recognition to having a back-up solution for GNSS as the source of PNT in the situations above, several potential technological solutions have been or are being developed to provide alternate position navigation and timing (A-PNT). While classical inertial sensors can provide the bandwidth and range, they are insufficient, and do not provide sufficient accuracy for approach and landing.

It is expected that the integration of quantum sensors into navigation systems could cover this gap, to achieve high accuracy and increasing resilience of trajectory-based operations.

Other advanced Quantum Sensing systems could also perform better in challenging environments where GNSS signals are weak or disrupted, such as:

- High-altitude airspace operations
- Underground or underwater locations
- Dense urban areas or mountainous regions

An additional Quantum Sensing technology-quantum timing (particularly those involving ultra-precise timing or optical clocks) has the potential to significantly enhance radar systems. Integrating versions of this into navigation systems could ultimately enable the detection of stealth or small objects, such as drones, at greater distances, and it can play a crucial role in counter-unmanned aircraft systems (counter-UAS) operations.

In the UK, researchers at the Quantum Technology Hub in Sensing, Imaging and Timing (QuSIT) are actively developing quantum-enabled radar systems. These systems are currently being tested from the rooftops of two university campus buildings, where they are used to track the movement of drones and other airborne objects to demonstrate how quantum timing can transform situational awareness in complex airspace environment.[22]

[22] Quantum-enabled radar - UK Quantum Technology Research Hub in Sensing, Imaging and Timing

Ultimately, Quantum Sensing could be integrated into UAS (drone) operations to significantly enhance their operational capabilities. By equipping drones with quantum sensors, they could achieve improved detection of a wider range of materials and environmental conditions, even in challenging or hard-to-access environments.

This advancement would enable drones to operate more effectively in scenarios where traditional sensors struggle such as dense urban areas or extreme weather conditions, making them more versatile for applications in environmental monitoring, infrastructure inspection, and search and rescue operations. It can also support real-time location tracking and improve situational awareness in congested airspace environments, making it a valuable tool for both civilian and defence aerospace applications.

Though Quantum Sensing is advancing practical use cases, particularly in aerospace, other elements of the application such as quantum timing are still in practical stages of early validation, but they are progressing rapidly and showing promising potential for real-world applications.[23]

In the UK, the UK Quantum Technology Hub in Sensing, Imaging and Timing (QuSIT) is working with industry and academia provide real-world use cases, scale up, and manufacture Quantum Sensing applications, whilst companies such as Infleqtion, BAE Systems, and QinetiQ are working to demonstrate how Quantum Sensing can be applied in practice, particularly in developing unjammable and unspoofable quantum-based navigation systems for commercial aviation.

Meanwhile, outside the UK, EU initiatives like the SESAR Horizon Europe programme have launched exploratory research calls aimed at integrating Quantum Sensing into air traffic management, especially for crewed aircraft and drone navigation. Together, these UK and EU efforts are accelerating the development, understanding, and adoption of Quantum Sensing in the aerospace sector.

Quantum Sensing: Challenges

Among all Quantum Technologies, Quantum Sensing is currently at the most advanced stage of technical development. It benefits from a strong foundation of proven use cases, along with substantial investment and commercial activity, particularly in sectors such as healthcare, defence, infrastructure, and built environment. However, whilst many applications have already been identified, predicting how the technology will evolve beyond defence and healthcare applications over the next decade remains challenging.

Temperature control remains a significant challenge in Quantum Sensing. These sensors often require advanced cooling systems to operate at peak performance. Although research has made notable strides in this area, maintaining the necessary thermal conditions continues to present supply chain and cost-related hurdles.[24]

Despite these challenges, Quantum Sensing technologies are already proving highly effective and are seeing growing adoption. However, for novel applications to gain traction, they must clearly address unmet needs and demonstrate distinct advantages over existing technologies, whether through enhanced sensitivity, greater cost-efficiency, or unique capabilities beyond the reach of conventional sensors.

[23/24] Exploring Quantum Sensing Potential for Systems Applications | IEEE

Potential timeline for development of Quantum Sensing in Aerospace:

0-5 years	5-10 years	10-15 + years
> Increased research between industry, hubs and academia. > Commercial prototypes of Quantum Sensing technologies have been promoted, including various sensor and imaging systems, some of which have already seen early real-world deployment. > Scaled down versions to improve integration and increase usability	> Quantum navigation systems, including clocks, independent of satellite signals may be deployed on aircraft. > Advancements in Quantum Sensing and imaging for defence may begin to find broader applications in civilian sectors. > Quantum Sensing across vital UK organisations such as the NHS (government target of 2030). Use cases and lessons learned may be transferable to other industries such as aviation.	> Broader adoption of Quantum Sensing and imaging techniques, either alongside or as replacements for classical technologies. > Integration into several modalities. e.g drones, cameras for autonomous vehicles, or monitoring real life air traffic in congested airspace areas. > Real time monitoring of energy consumption. e.g fuel combustion, or battery diagnostics for electric aircraft.

Illustration of what Quantum Sensing could look like in Aerospace:

Aerospace 2035...

By 2035, the skies above smart cities, rural logistics corridors, and across border zones are filled with millions of automated drones. These drones perform critical tasks ranging from on-demand deliveries and emergency response to surveillance and defence missions, navigating dense, urban environments filled with skyscrapers, complex infrastructures, and dynamic air traffic.

To manage this complexity, SkyLoad has deployed SkyLoad Q a next-generation, quantum-sensor-enhanced platform that enables real-time decision-making, site identification, fleet coordination, and threat detection at a global scale. Powered by Quantum Sensing, SkyLoad Q delivers precision, resilience, and situational awareness in even the most challenging environments.

SkyLoad receives a BVLOS (Beyond Visual Line of Sight) food delivery request for a high-density neighbourhood in London during peak commute time. The destination is a shared-use building with strict access protocols and limited GNSS reliability due to signal interference.

Within seconds, SkyLoad QNet leverages its quantum sensors to pinpoint the exact delivery location, verify access permissions, and guide the drone through a safe, efficient flight path executing a seamless, secure drop-off without human intervention.

3. Quantum Communications

Current Status: TRL 6-8

Quantum communication is relatively more mature than other Quantum Technologies, with several UK-based pilots underway via national test beds. It involves creating quantum channels by using fibre networks or satellites to transmit information. This is primarily used for QKD, which enables a secure way to distribute symmetric keys for further communication via a classical channel. This technology is particularly relevant in defence, finance, space, and cybersecurity, and is being explored in aerospace for tamperproof communications and enhanced navigation systems, complementing measures provided by PQC.

In the UK, the Quantum Communications Hub, part of the National Quantum Technologies Programme, focuses on advancing and commercialising QKD-based applications. In contrast, the U.S. has expanded its quantum networking efforts through the CHIPS and Science Act of 2022, which supports R&D and standardisation in quantum communication infrastructure.

Quantum communication is advancing quickly in the aerospace sector. One notable example is the European Space Agency's partnership with Arqit to launch QKDSat, a satellite-based QKD system. QKDSat enables the secure distribution of symmetric encryption keys via a cloud-based platform, requiring minimal computational resources (under 200 lines of code).

By leveraging quantum physics, it ensures that encryption keys remain inaccessible to eavesdroppers. A network of QKDSat satellites will eventually enable the exchange and distribution of secure encryption keys to countless locations and devices. By generating keys from high-quality random sources and distributing them via the cloud, this system is expected to significantly enhance resilience against future cyber threats.

Quantum Communications, particularly those involving satellite-based systems hold significant promise for enhancing the capabilities of aerodromes. This potential is being actively explored at the Errol Aerodrome Optical Ground Station (OGS) in the UK, which serves as a hub for research teams working to establish quantum-secure links with satellites and communication payloads.[25]

Despite the growing interest in QKD technologies, the UK's National Cyber Security Centre (NCSC) does not endorse their use for government or defence applications.[26] The primary concern is that QKD does not provide authentication (establishing the identity of a person).

The NCSC advises organisations considering QKD to implement quantum-resistant authentication mechanisms, such as PQC. PQC algorithms are designed to withstand attacks from quantum computers and can be integrated with QKD to form a more comprehensive security solution. For this reason, the NCSC recommends prioritising PQC over QKD for high-assurance environments.

Potential timeline for development of Quantum Communications in Aerospace:

0-5 years	5-10 years	10-15 + years
> Ongoing trials on QKDs in aviation. > Use cases led by defence and financial sectors for the secure transfer of data.	> Additional authenication mechanisms to compliment QKDs. > Satellite based QKDs for secure communications between countries where fibre-optic connections are not possible. > Increased specialised variations of QKDs for sectors (e.g military, government, aviation and healthcare).	> Intergration with existing infrastructure such as fibre optic networks. > Cloud providers may offer quantum-secured communication services, making QKD more accessible to a wider range of users such as vertiport operators, drones, eVTOLS etc. > QKDs evolve to personal gadgets which streamlines communications between passengers and services providers.

Illustration of what Quantum Communications could look like in Aerospace:

Aerospace 2035...

In the year 2035, major international airports and aerodromes have integrated QKD and PQC systems into their core infrastructure to ensure ultra-secure communications across all flight operations.

At the terminal, biometric verification has become seamless. Security personnel access encrypted passenger profiles, including facial recognition and travel history, before travellers reach the gate. Meanwhile, flight attendants carry quantum-encrypted tablets that instantly verify boarding details and passenger information without risk of data exposure.

In the air, the cockpit remains securely connected to a vast network of ground stations, nearby aircraft, airports and autonomous ground operations. Through quantum-secured channels, pilots exchange:

> Real-time monitoring and diagnostic reports.

> Encrypted voice and data communications with air traffic control.

> Autonomous coordination with eVTOLs, drones, and higher-airspace operations.

Even emergency protocols are quantum-encrypted, ensuring no delay or interference in crisis communications.

By 2035, quantum-security is an invisible infrastructure that underpins trust in every flight, every airport, and every connection across the skies.

Quantum Communications: Challenges

QKDs offers a promising method for achieving highly secure communication, leveraging the principles of quantum mechanics. However, several significant challenges hinder its widespread deployment. One of the foremost obstacles is the need to develop reliable and scalable quantum-hardware. Quantum systems are inherently fragile and highly sensitive to environmental noise, which makes maintaining stable and efficient transmission particularly difficult especially over long distances. Currently, limitations in hardware and engineering mean that quantum information can only be reliably transmitted over relatively short ranges. In the UK, for example, QKD has been successfully demonstrated between cities up to around 410km, but extending this capability to international distances remains a major technical hurdle.[27]

QKD technologies within government agencies and other safety critical organisations remains limited, partly due to the need for complementary authentication systems that QKD alone does not provide. This has led to hesitation around its broader implementation. Additionally, the cost of deploying QKD infrastructure alongside the necessary authentication mechanisms can be prohibitively high, further contributing to cautious uptake.

[27] Researchers demonstrate the UK's first long-distance ultra-secure communication over a quantum network | University of Cambridge

4. Post Quantum Cryptography

Current Status: TRL 7-8

One of the main theorised algorithms for quantum computers is a factorisation algorithm called Shor's Algorithm.[28] Since its theorisation, the algorithm has had multiple proof of concepts at a small scale.[29] The purpose of the algorithm is factorising composite numbers into their prime factors in polynomial time. While this may seem harmless on the surface, this can be utilised to crack one legacy and two current standards for Public Key Infrastructure (PKI).[30]

Almost all modern internet security is built on PKI and its ability to encrypt traffic on insecure connections. Therefore, there is an initiative to upgrade all current PKI algorithms to quantum resistant algorithms before the first Cryptographically Relevant Quantum Computer (CRQC) is made. Current projections say this is likely by 10-15 years in the future.[31] However, adversaries are likely to be downloading encrypted data, to then decrypt it when a CRQC is available; this is known as a harvest now, decrypt (HNDL) later attack.

HNDL attacks are most likely to be performed first by nation states and then secondly by large criminal organisations. As with their standard operation patterns, nation states will likely use these attacks political gain and large criminal organisations will use them for financial gain. With these two threat actor types, safety critical aviation systems are unlikely to be a target due to their lack of political or financial opportunities. Corporate aviation systems, however, will likely be a target as there is a large financial incentive to steal intellectual property, and personally identifiable information.

Looking at the aviation supply chain we have found that the PKI is primarily used within common security protocols such as

Transport Layer Security (TLS) and IP Security (IPSec). These protocols are very common in the corporate side of the aviation industry but are much rarer in the security or safety critical side. In the large aircraft sector, we have found the use of PKI in systems such as Electronic Flight Bags (EFB's), which use TLS to connect to their update servers securely. This connection will use PKI to connect to an update server securely.

Much of aviation's safety critical infrastructure still uses analogue systems and as such not encrypted. This means they will not at risk from quantum enabled attacks; however, they are more vulnerable to more common attacks such as spoofing. Consequently, ICAO have begun an initiative known as the ICAO Trust Framework, which is suggesting digitising and encrypting safety critical aviation systems. The most popular style of encryption solution would be PKI.

Since 2016 NIST has been creating a set of public key cryptographic standards that are resistant to all know quantum attacks, so as to replace the current PKI standards. In 2024, they released 3 standards: Module Lattice Based Key Encapsulation Mechanism Standard (FIPS 203), Module Lattice Based Digital Signature Standard (FIPS 204), and Stateless Hash Based Digital Signature Standard (FIPS 205). A future 4th digital signature standard (FIPS 206) is currently scheduled for 2027.[32] FIPS 203 is the most popular of the standards and is likely to see wide adoption including in the UK.[33]

[28] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer | Academic Paper
[29] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance | Academic Paper
[30] Recommended Cryptographic Standards | NCSC [31] 2023 Quantum Threat Timeline Report | Global Risk Institute
[32] NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption | NIST
[33] Next Steps Preparing for Post-Quantum Cryptography | NCSC Whitepaper

The National Cyber Security Centre (NCSC) has released their recommended timescale for large organisations and operators of critical national infrastructure.[34] Within their guidance there are 3 key milestone dates:

2028

- Define your migration goals
- Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)
- Build an initial plan for migration

2031

- Carry out your early, highest-priority PQC migration activities
- Refine your plan so that you have a thorough roadmap for complete migration

2035

- Complete migration to PQC of all your systems, services and products

There have also been discussions on the weaknesses of the PQC algorithms. One of its weaknesses is that the algorithms assume a source of true randomness is used for key generation.[35] Current technology offers pseudo-random number generation, which while resistant to initial CRQC machines, it may become susceptible to more mature quantum computers. Fortunately, sources of Quantum Random Number Generation (QRNG) are being worked on by multiple organisations and are beginning exploring the early onset applications within civil aviation.

The other key challenge around the PQC standard algorithms, is their capacity to remain resistant to quantum and classical attacks. As with much of cryptography, it is unknown how long a cryptographic algorithm will remain secure before it is broken by new technology or cracked by a weakness. As such, we cannot expect the PQC standard algorithms to be a permanent solution and should prepare systems for future upgrades.

[34] Timelines for Migration to Post-Quantum Cryptography | NCSC
[35] Randomness in PQC | Quantum Dice