VOLUME 54 / MARCH 2026

WORLD AIR NEWS

CONNECTING SKIES • BRIDGING CONTINENTS

CERTIFYING CHANGE
OVERSIGHT IN MOTION

AUTONOMY AS TESTBED

SOFTWARE-DEFINED SKY
SOFTWARE OPERATIONS

COVER IMAGE : THE MIGHTY DASSAULT FALCON 10X © DASSAULT

MORE PROVEN: THE PC-12 PRO IS HERE!

Featuring the world's most reliable engine, the Pratt & Whitney Canada PT6.
Proven has been redefined – introducing the brand-new PC-12 PRO.

Pilatus Centre SA
Authorised Sales Centre

Crafted in Switzerland

pilatus-aircraft.com/southernafrica

DISCIPLINED DESIGN, DELIVERED

The Airbus A220 reflects March's focus on disciplined operational evolution. As a clean-sheet design, the aircraft integrates advanced flight deck systems, refined aerodynamics and efficiency-driven engineering into a platform built for contemporary airspace complexity. It is not defined by radical change, but by deliberate refinement — systems working cohesively to support structured crew decision-making and sustainable performance margins. In an industry where incremental improvement often delivers the greatest operational stability, the A220 represents design maturity aligned with procedural integrity.

Images Courtesy of: Airbus

OFFICIAL JOURNAL OF:– Commercial Aviation Association of Southern Africa, The Airlines Association of South Africa, The Association of South African Aircraft Traders, Association of Training Organisations of South Africa, Aerodromes & Airports Association of South Africa, Association of Aviation Maintenance Organisations, South African Society of Aerospace & Environmental Medicine, Helicopter Association of Southern Africa, Aircraft Owners & Pilots' Associations of Southern Africa, Airside Operators, Association of South Africa, South African Aerial Applicators Association, East African Commercial Aviation Association, African Airline Association (AFRAA) Media Partner.

CONTACTS

PUBLISHER WORLD AIRNEWS PTY LTD
15 Jacaranda Drive, Craigavon AH, Sandton,2192
Telephone: +27 11 465 7706 / 083 378 2060
info@worldairnews.co.za

EDITORS
Joan Chalmers
Email: joan@worldairnews.co.za

Joey Schulz - Sub Editor
Email: joey@worldairnews.co.za

Keith Fryer -Technical Advisor
Email: keith@worldairnews.co.za

OPERATIONS & ENQUIRIES
Judi Rodokanakis
Email: judi@worldairnews.co.za

ACCOUNTS
Krystyna Zanike Evans
Email: krys@worldairnews.co.za

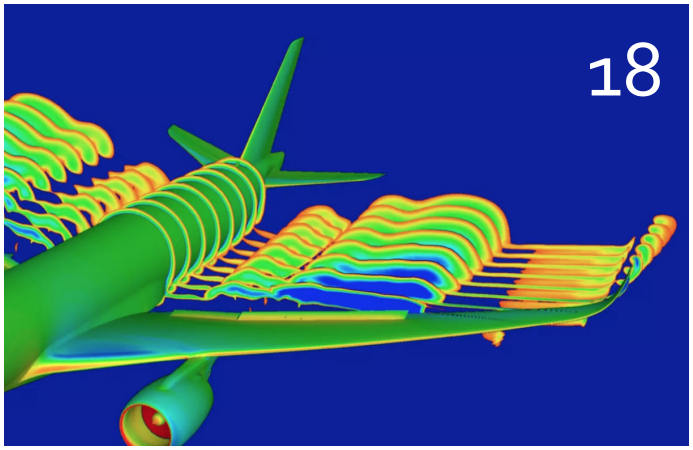
BUSINESS DEVELOPMENT/ SOUTH AFRICA
Hes Kiggen
Email: hes@worldairnews.co.za

Jimmy Skosana
Email: jimmy@worldairnews.co.za

BRITAIN / EUROPE BSP
Sally Passey
Email: sally@worldairnews.co.za

RUSSIA - MOSCOW
Yury Laskin
Email: yury@worldairnews.co.za

DISTRIBUTION CHANNELS
WEBSITE: www.worldairnews.co.za
SOCIALS: Facebook, LinkedIn, Instagram, Twitter, Magzter.
DIRECT MAIL: Monthly emailer to Subscribers and Aviation Sector Specialists.
ON -DEMAND PRINTING: We only print what is needed.



AIR WORLD NEWS

CONTENT

34 CYBER, RISK & MISSION SYSTEMS

Protection, resilience and mission capability increasingly depend on software integrity. These articles examine cybersecurity as infrastructure, business aviation's certification realities, and forward-looking system predictions.

40 AUTONOMY AS PROVING GROUND

Uncrewed aviation is not peripheral — it is the systems laboratory for the future of flight. This section positions autonomy as the operational test bed shaping certification, safety logic and architecture.

42 DIGITAL MARKETS & INFRASTRUCTURE

The commercial layer of digital aviation — cloud, enterprise software, mission systems and infrastructure — reflects where investment and integration are accelerating across the aviation ecosystem..

50 CLOSING PERSPECTIVE

Technological change ultimately collides with organisational culture. This closing reflection considers margin erosion, normalisation of deviation and the evolving role of the systems manager in a software-defined aviation era.


No SIM
LIBR
Route
Pubs
LIRF
REF
STAR
APP
TAXI
SID
ATHENS FIR
LGGG
TRL (TRIPOLIS)
48 NM → EKTOS
ACC 123.72 123.82
AIRSPACE
ATHENS TMA
FL460
1000
Airspace Speed
SPEED RESTRICTIONS WITHIN ATHEN...
AIRSPACE
ATHENS TMA (C)
FL195
1000
13:24
LOW IFR 787-9
LIRF
OMDB
North Up
LGLR
KFN
LGRX
TRL
UM601
FL250
EKTOS
Wx
L FIR
LMMM UIR
LMMM FIR
©WAN

WHEN AWARENESS IS NOT ENOUGH

One of aviation's most persistent blind spots is not the absence of data, but the space between recognising risk and responding to it. Modern operations generate vast amounts of information.

Exceedances are logged, deviations recorded, audits completed and trend reports reviewed. Yet operational margins can quietly narrow while organisations take comfort in the fact that nothing has yet gone wrong.

Risk identification alone does not produce change. Intervention depends on clear ownership, aligned culture and leadership prepared to act before external pressure forces a response. Without that, insight becomes documentation rather than decision.

Infrastructure choices influence resilience long before aircraft taxi. Training philosophy shapes whether procedures are treated as disciplined standards or flexible guidance. Executive leadership determines whether safety intelligence prompts corrective movement or settles into archived reporting. Digital platforms enhance visibility, but visibility without authority rarely alters outcomes.

Across fleet renewal, airspace protection, infrastructure investment and governance transitions, the same structural question emerges: when indicators are visible, who is responsible for moving first? In highly regulated environments, accountability can diffuse across committees, departments and oversight layers. Risk may be acknowledged and discussed, yet remain unresolved because responsibility is shared but not owned.

Over time, tolerance shifts. What once appeared abnormal begins to feel routine. The routine becomes acceptable.

Aviation remains one of the most procedurally governed industries in the world, and rightly so. But structure alone does not guarantee resilience. Data without intervention becomes background noise. Safety management systems and predictive analytics provide powerful tools, yet they cannot substitute for decisive governance.

Safety has never depended solely on technology. It has depended on the willingness to act before consequence compels reaction.

As fleets modernise and operations become increasingly digitised, the underlying principle remains unchanged. Awareness is the starting point, not the solution. Sustainable resilience is built not on how effectively risk is described, but on how consistently it is addressed.

THE SOFTWARE-DEFINED SKY

When software becomes the primary safety system, what is the aircraft?

For more than half a century, aviation safety has been built on mechanical reliability, procedural discipline and pilot judgement. Today, an additional layer has become central: software logic. From flight-envelope protections to uncrewed aircraft autonomy and data-driven fleet oversight, safety margins are increasingly defined in code. As software becomes the primary mediator between pilot, platform and environment, the question is no longer whether aviation is digital — but what an aircraft becomes when software governs its limits.

From Mechanical Limits To Coded Limits

Modern commercial aircraft already operate within software-defined boundaries.

Fly-by-wire systems, first introduced into commercial service in the late twentieth century, replaced direct mechanical linkages with electronic signalling and control laws. Flight-envelope protections embedded in those control laws prevent pilots from exceeding structural or aerodynamic limits under normal operating modes. In such architectures, the aircraft's behaviour is interpreted and filtered by software before control surface commands are executed.

This does not remove the pilot from authority. It places the aircraft's response within predefined computational boundaries.

The shift is subtle but fundamental. Safety margins are no longer solely physical tolerances. They are design decisions expressed in algorithms.

Certification In A Software Environment

Civil aviation has not treated this transition lightly.

Software used in airborne systems is governed under rigorous assurance frameworks, most notably through standards such as DO-178C and associated regulatory guidance issued by authorities including the FAA and EASA. Changes to certified software are subject to structured impact analysis, re-verification and documentation requirements.

The existence of formal Change Impact Analysis guidance reflects a central reality: when software defines behaviour, any modification has potential safety implications.

In a hardware-dominant era, components were replaced. In a software-defined era, behaviour itself can be updated. Certification must therefore determine not only whether a system works — but whether its logic remains within an acceptable safety envelope over time.

The Drone Domain: Software As Primary Authority

Nowhere is this shift more visible than in uncrewed aircraft systems (UAS).

In most drones, stability, navigation, contingency management and geofencing are governed by onboard software from inception. There is no direct mechanical fallback equivalent to traditional flight control.

Autonomy logic interprets sensor inputs, fuses data and determines aircraft response.

Regulators have responded with risk-based frameworks such as EASA's Specific Operations Risk

Assessment (SORA), which evaluates operational risk through system performance and mitigation measures rather than through pilot certification alone.

This is significant. In crewed aviation, safety has historically been distributed between pilot skill, mechanical redundancy and procedural oversight. In UAS operations, autonomy logic itself becomes a primary safety layer.

Moreover, the drone ecosystem has introduced another pressure point: iteration speed. Software updates in some UAS fleets can occur far more rapidly than in conventional transport-category aircraft programmes. Each update potentially alters behaviour, requiring oversight mechanisms capable of distinguishing operational refinement from safety-critical change.

Drones therefore represent the first aviation domain in which:

- Software is the primary flight control authority
- Post-deployment behaviour can change relatively quickly
- Autonomy logic directly defines separation, obstacle avoidance and contingency response

They are not an outlier. They are a preview.

Connected Fleets And Data-Driven Safety

Parallel to autonomy, another transformation is underway: fleet-level safety intelligence.

Programmes such as the FAA's Aviation Safety Information Analysis and Sharing (ASIAS) system and EASA's Data4Safety initiative are built on large-scale operational data analysis. The objective is to identify systemic risk patterns before they manifest as accidents.

This represents a shift from reactive investigation to proactive risk modelling.

In such environments, safety envelopes are not static. They are informed by data trends, operational deviations and emerging hazards identified across fleets. The aircraft becomes part of a data ecosystem rather than a standalone entity.

However, data-driven oversight does not replace design assurance. Monitoring can detect risk drift, but it cannot compensate for flawed system logic at design level. The integrity of software architecture remains foundational.

Autonomy, Detect-And-Avoid And System Authority

As uncrewed and increasingly automated systems integrate into shared airspace, standards bodies such as RTCA have developed performance frameworks for Detect-and-Avoid (DAA) and command-and-control links.

In this model, separation assurance — historically managed by pilot visual scanning and air traffic control — becomes a function of algorithmic detection thresholds, latency limits and link integrity.

The safety margin is no longer purely procedural. It is mathematical.

Performance standards define acceptable probabilities of failure, response timing and data integrity requirements. Compliance determines whether autonomy is considered airworthy within a given operational context.

Continuous Certification Pressure

The more software defines behaviour, the more certification becomes continuous rather than episodic.

Traditional airworthiness was centred around initial type certification and periodic inspection. In a software-defined system, oversight must consider:

- Configuration management
- Software version control
- Cybersecurity integrity
- Data validity
- Behavioural drift after updates

This does not imply regulatory instability. It implies regulatory evolution.

Authorities increasingly recognise that assurance must extend across the lifecycle of digital systems, not merely their entry into service.

What, Then, Is The Aircraft?

If safety limits are expressed in control laws,if separation is governed by detect-and-avoid algorithms,if behaviour can be altered through software revision,if risk identification depends on fleet-wide data analytics, then the aircraft is no longer defined solely by its airframe and propulsion.

It is defined by an integrated architecture:

- Airframe
- Sensors
- Control software
- Data links
- Update governance
- Certification artefacts
- Operational monitoring

The physical platform remains critical. But safety authority increasingly resides in software integrity.

A Structural Transition, Not A Trend

This is not a sudden revolution. It is a gradual structural transition.

Crewed aircraft have operated under software mediation for decades. Drones have accelerated the shift by placing autonomy at the centre of control. Fleet analytics have expanded the safety system beyond the aircraft itself.

The question is not whether aviation will remain hardware-based or become software-based. It is how effectively the industry governs software as a safety-critical system.

When code defines the limits, certification defines the boundaries of trust.

BOEING MQ-25 STINGRAY: CARRIER-BASED AUTONOMY IN OPERATION

Designed for operations from one of aviation's most demanding environments, the Boeing MQ-25 Stingray demonstrates how autonomous systems are being validated in complex, high-risk operational domains.

The Boeing MQ-25 Stingray is an unmanned aerial refuelling aircraft developed under the United States Navy's Carrier-Based Aerial Refueling System (CBARS) programme. It is intended to provide aerial refuelling support to carrier air wing aircraft including the F/A-18 Super Hornet, E-2D Hawkeye and F-35C Lightning II.

The aircraft first flew on 19 September 2019 and has since conducted mid-air refuelling tests, demonstrating the feasibility of unmanned tanker operations.

In August 2018, Boeing was selected as prime contractor for the programme under a contract initially valued at approximately US $805 million. Fleet expansion is planned over the coming decade.

The United States Navy intends to begin integrating the MQ-25 aboard aircraft carriers from 2026, with ongoing flight testing preceding operational deployment.

Autonomy In A High-Risk Environment

Aircraft carrier operations are widely regarded as among the most complex in aviation. Launch and recovery cycles require precise timing, tightly controlled deck movement and resilient communications.

The MQ-25 has been developed with advanced autonomous systems enabling automated taxiing, take-off, flight profile execution and approach procedures within this operationally intensive environment. These capabilities allow the aircraft to operate alongside crewed platforms while maintaining strict integration within carrier deck procedures.

Its development provides a visible example of software-centric aviation systems replacing onboard human input in defined mission roles.

Manned-Unmanned Teaming

The MQ-25 is designed to operate as part of a manned-unmanned team, performing refuelling missions that would otherwise require crewed tanker or strike aircraft to assume the role.

Flight tests have demonstrated the aircraft's ability to refuel carrier-based fighters, allowing those platforms to focus on primary operational missions. This approach reflects a broader trend in defence aviation towards distributed mission architectures supported by autonomous systems.

Mission Control And Command Architecture

Operational deployment includes mission planning and execution from shore-based or carrier-based mission control stations.

The Unmanned Carrier Aviation Mission Control System (UMCS) integrates hardware, software and communications networks to enable remote and beyond-line-of-sight operations. This command-and-control architecture forms part of a broader evolution towards networked, software-defined aviation systems.

Technical Characteristics

The MQ-25 is powered by a Rolls-Royce AE 3007N turbofan engine.

Its refuelling system enables the transfer of fuel to multiple fighter aircraft during a single mission. In addition to its primary tanker role, the aircraft is expected to support secondary intelligence, surveillance and reconnaissance (ISR) capabilities.

The programme represents an evolution from earlier carrier unmanned aircraft concepts, including the UCLASS initiative.

Defence Development And Civil Relevance

Although developed for military use, the MQ-25 reflects a recurring pattern in aviation technology adoption. Autonomous systems and integrated mission software are often validated first in defence environments characterised by high operational complexity and risk tolerance.

Such developments frequently influence subsequent civil aviation applications, including autonomous logistics platforms, surveillance operations and extended-endurance unmanned systems.

In this context, the MQ-25 Stingray illustrates how carrier aviation is serving as a proving ground for software-defined operational capability.

AIR TRAFFIC, AIRSPACE & SYSTEM ORCHESTRATION

When Airspace Becomes Computed

For most of aviation's history, airspace has been managed through observation, procedure and voice coordination. Controllers monitored radar screens, issued clearances and maintained separation through structured spacing and judgement.

Today, that visible layer remains. Beneath it, however, a dense digital infrastructure is reshaping how the sky functions.

Modern airspace is no longer defined solely by sectors and radio frequencies. It is modelled, predicted and continuously recalculated by software systems integrating surveillance data, trajectory forecasting and network-wide traffic flow management.

Airspace is still controlled by humans. Increasingly, it is structured by software.

From Radar to Data Fusion

Traditional air traffic control relied primarily on ground-based radar and voice communication. While these remain core components, contemporary air traffic management (ATM) systems integrate multiple surveillance sources, including:

- Primary and secondary radar
- ADS-B (Automatic Dependent SurveillanceBroadcast)
- Multilateration systems
- Satellite-derived surveillance inputs

Images Courtesy of: StockCake

These data streams are fused within flight data processing systems that continuously compute aircraft trajectories, predicted separation points and conflict alerts.

Airspace is therefore not merely observed. It is mathematically projected minutes ahead.

Thales: Integrated ATM Architecture

Thales is one of the principal global suppliers of ATM infrastructure, providing surveillance systems, digital towers, flight data processing systems and decision-support tools.

Its platforms integrate:
- Real-time surveillance data
- Automated conflict detection
- Trajectory-based planning tools
- Remote digital tower environments

Digital tower implementations, for example, allow controllers to manage airport operations using high-definition visual sensor arrays and software-processed imagery rather than direct line-of-sight observation.

The shift is not toward automation replacing the controller. It is toward computational support enhancing situational awareness and predictive capacity.

Indra: Civil–Military Integration

Indra supplies civil and military ATM platforms across multiple regions, including Europe, Latin America and Asia.

Its systems support:
- Area control centres
- Surface movement radar systems
- Civil–military airspace coordination
- Command and control integration

Modern airspace increasingly requires dynamic sharing between civil traffic flows and military operations.

Software platforms enable real-time reallocation of restricted zones, flexible use of airspace and integrated surveillance across domains.

Airspace flexibility, once negotiated procedurally, is now structured through digital system logic.

Frequentis: The Communications Backbone

While surveillance and trajectory modelling shape airspace awareness, communications infrastructure sustains separation authority.

Frequentis provides safety-critical voice communication systems and controller working positions used by ANSPs worldwide.

Its platforms support:
- Controller–pilot data link communications (CPDLC)
- Voice over IP migration in ATC environments
- Integrated command and control systems
- Remote tower communication networks

As airspace digitises, voice circuits evolve into IP-based, redundant digital networks. Communication resilience becomes a software-governed variable within the airspace ecosystem.

Separation assurance depends not only on radar accuracy, but on communication system integrity.

Skyguide: Operational Reality

Skyguide, the Swiss Air Navigation Service Provider, offers a practical example of software-driven airspace control.

Managing complex terrain, dense European traffic flows and civil–military integration, Skyguide operates within an environment shaped by SESAR modernisation initiatives.

Its systems incorporate:
- Advanced conflict detection and short-term trajectory prediction
- Integrated civil–military coordination platforms
- Network-wide traffic flow optimisation

Controllers remain central decision-makers. However, their working environment is defined by predictive algorithms, digital coordination tools and structured traffic modelling.

The controller's authority remains human. The margin for safety is increasingly computationally supported.

The Orchestrated Sky

The transition underway is not toward autonomous airspace. It is toward orchestrated airspace.

System-wide information management (SWIM), trajectory-based operations and digital data exchange frameworks promoted under SESAR and NextGen initiatives reflect this shift.

Airspace capacity is modelled dynamically. Conflict alerts are computed.

Traffic flows are optimised algorithmically. The sky is no longer a static volume divided by fixed lines. It is a continuously recalculated network environment.

Aircraft may be software-defined. Airspace is becoming software-orchestrated.

The work of companies such as Thales, Indra and Frequentis, and the operational realities demonstrated by ANSPs such as Skyguide, illustrate a structural change in aviation governance.

Controllers still issue clearances. Pilots still respond. Human judgement remains decisive.

Yet beneath that exchange lies a digital architecture computing separation, predicting congestion and shaping how aircraft move through the sky.

Airspace is still managed. Increasingly, it is computed.

OPERATING THE AIRPORT AS A SYSTEM

World Airnews Interview with Nkululeko Mhlaba

Unlocking capacity through integrated digital infrastructure

African airports are under growing pressure. Passenger volumes continue to rise, yet large-scale capital expansion remains constrained by funding cycles, regulatory complexity and long construction timelines.

For Nkululeko Mhlaba, the constraint is not primarily physical infrastructure. It is operational architecture.

In a conversation focused on digital infrastructure and airport operations, he argues that the next gains in throughput and resilience will not come from more concrete — but from better coordination, visibility and decision logic.

"The primary constraint is not runway or terminal size, but the efficiency of core operational processes."

Software Vs Steel

***World Airnews*: Many African airports are operating close to design capacity. What operational constraints are proving hardest to solve through traditional infrastructure alone?**

Nkululeko Mhlaba: Many airports are already close to their original design capacity while traffic continues to grow at approximately 5–7% per year. The primary constraint is not runway or terminal size, but the efficiency of core operational processes such as aircraft turnaround, gate assignment and passenger processing. These processes are often managed in silos, which limits throughput. Improving coordination and decision-making across these functions can unlock 15–20% additional capacity without major infrastructure investment.

This is where the distinction becomes clear. Infrastructure expands space. Software expands coordination.

Decision-Making Under Complexity

***World Airnews:* Where does software make the most immediate difference in the African operating context?**

Mhlaba: Software delivers immediate value where operational decisions need to be adjusted dynamically — gate management, turnaround coordination and baggage handling. Real-time operational platforms have reduced gate conflicts by up to 30%. However, impact is constrained where legacy systems are poorly integrated or where operational processes have not been redesigned. Software is most effective when it supports clearly defined workflows and decision rights.

In complex airport ecosystems, the issue is not lack of data. It is fragmented visibility.

Information gaps typically emerge during operational handovers between airlines, ground handlers and airport control centres. When stakeholders operate on partial or delayed information, small disruptions propagate quickly. Integrating operational data into a shared view allows earlier identification of conflicts and can reduce knock-on delays by around 25%.

Legacy Systems And Hidden Risk

Many airports continue operating on ageing systems that function adequately under normal conditions. The vulnerability becomes visible during peak demand or disruption.

***World Airnews:* What risks are underestimated when digital modernisation is delayed?**

Mhlaba: Ageing systems introduce limited visibility, manual workarounds and delayed response times.

These increase the likelihood of operational errors and extended recovery periods. Modernising systems improves situational awareness and supports faster, more consistent decision-making during high-pressure situations.

In this context, digital modernisation is not primarily about efficiency. It is about operational resilience.

From Reactive To Predictive Operations

The language of "predictive operations" is increasingly used across aviation. In practical airport terms, it is less abstract than it sounds.

***World Airnews:* What does predictive mean for an operations team on a busy day?**

Mhlaba: Predictive operations use historical trends and current data to forecast potential constraints — staffing shortfalls, gate conflicts — before they occur. This allows teams to intervene earlier and adjust plans. Airports applying predictive approaches usually see a 15–25% reduction in operational disruptions. Real-time visibility also changes disruption management. Access to live passenger flow data or equipment availability enables proactive staff reallocation, reducing congestion and recovery times by approximately 20% compared with reactive models.

Software, in this environment, does not remove human decision-making. It reshapes its timing.

Data Without Overload

Airports already generate vast volumes of data. The risk is that digital platforms add complexity rather than clarity.

Mhlaba: Preventing overload requires focusing on a limited set of operationally relevant metrics. Systems should highlight exceptions and trends requiring action rather than presenting raw data. Clear dashboards and prioritised alerts ensure data supports decision-making rather than overwhelming it.
This is where digital maturity becomes critical. More data does not equate to more intelligence. Governance matters.

Local Execution In African Contexts

Digital platforms may be globally designed, but airport operations are locally specific.

Staffing models, regulatory environments and infrastructure constraints differ significantly. When implementation does not account for these realities, adoption drops and expected efficiency gains can fall by 30–40%.

Successful deployment aligns technology with operational procedures and training requirements. Digital architecture cannot be imported wholesale. It must be adapted.

Measuring What Matters

Efficiency metrics alone do not capture transformation.

***World Airnews*: How should airport executives measure genuine improvement?**

Mhlaba: Beyond efficiency, success should be assessed through operational reliability and recovery performance — on-time departures, reduced turnaround variability and faster recovery from disruptions.

Resilience, not just speed, becomes the defining metric.

What Changes — And What Remains Human

Over the next five years, software will increasingly support demand forecasting, resource allocation and stakeholder coordination.

Human decision-making, however, remains central in managing exceptions, passenger interactions and complex trade-offs.
The transformation is not about removing people. It is about giving them earlier, clearer visibility into system-wide constraints.

Software As Operational Authority

Airport capacity has traditionally been associated with physical expansion — longer runways, larger terminals, additional gates.

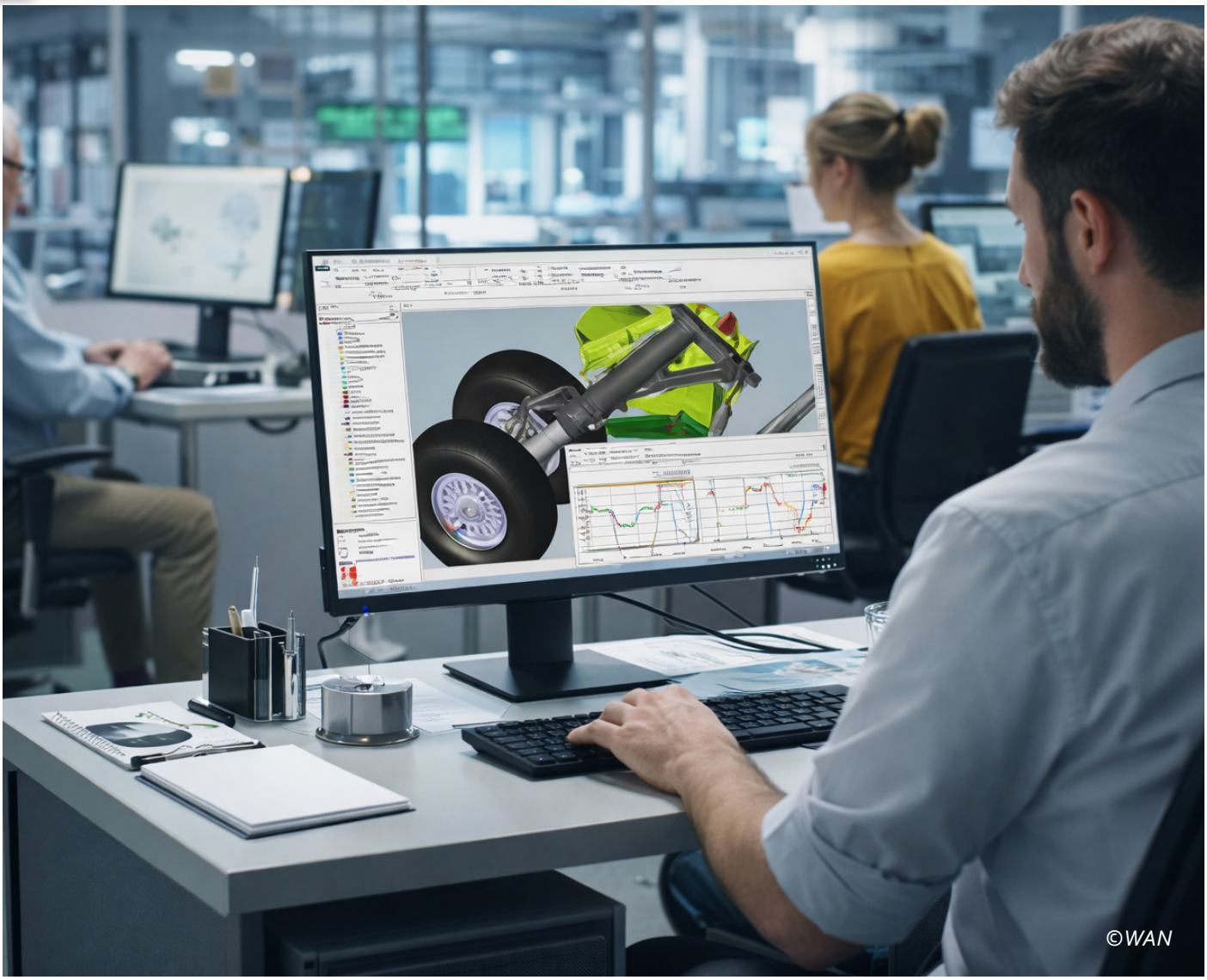
Yet across many African contexts, the next layer of capacity lies within the existing footprint.

Through shared operational data, predictive modelling and coordinated decision architecture, software increasingly governs how efficiently that footprint performs.

In this sense, the airport — like the aircraft and the factory — is becoming a software-defined environment.

The concrete remains in place. But authority is moving into code.

Nkululeko Mhlaba is the Chief Executive Officer of Phungela, an ISO-certified South African enterprise technology and digital transformation firm. He leads the company's work in digital infrastructure, systems integration and data-driven operational platforms across complex environments. With a focus on Africa-specific realities, Mhlaba advocates practical technology deployment that strengthens airport coordination, governance and resilience. His approach positions software as operational architecture — enabling visibility, accountability and measurable performance improvement.



THE QUIET RISE OF AVIATION SOFTWARE ARCHITECTS

Aviation safety has traditionally had visible custodians — captains, chief engineers, certification authorities and test pilots. Today, however, the individuals defining aircraft behaviour increasingly operate far from the flight deck. The people shaping modern aviation safety may never touch an aircraft control column.

Safety Authority Moves to Code

Modern aircraft are governed by software layers that determine flight control laws, navigation management, sensor fusion, health monitoring and data integration.

These functions are not peripheral enhancements; they are structural determinants of how the aircraft behaves in normal and abnormal conditions. Safety-critical software is developed under rigorous standards such as RTCA DO-178C and its European counterpart, EUROCAE ED-12C.

Within this framework, software leads are responsible for:

- Assigning Development Assurance Levels (DAL A–E) according to failure severity
- Maintaining strict requirements traceability
- Ensuring independence in verification and validation
- Conducting structural coverage analysis

Their task is not to innovate features. It is to engineer behavioural certainty under failure conditions.

In effect, safety authority increasingly resides within requirements documentation, verification matrices and assurance artefacts rather than physical handling characteristics alone.

Certification as a Design Discipline

Certification-facing code architects translate operational concepts into structures that regulators can evaluate and approve.

Their work intersects directly with authorities such as the Federal Aviation Administration and the European Union Aviation Safety Agency. Responsibilities typically include:

- Functional Hazard Assessments (FHA)
- Preliminary and System Safety Assessments (PSSA and SSA)
- Redundancy strategy design
- Partitioning logic within integrated modular avionics
- Definition of fail-safe and fail-operational behaviours

These architects determine how systems degrade when faults occur. Their decisions influence whether a malfunction results in manageable workload or cascading operational complexity.

Certification is therefore not a compliance afterthought. It is an architectural discipline shaping the aircraft from inception.

Assuring Autonomy

Where advanced automation and autonomy are introduced, the assurance burden intensifies. The central question shifts from functionality to trustworthiness under uncertainty.

Autonomy safety case designers construct structured arguments demonstrating that systems meet acceptable risk thresholds within defined operational design domains. Their work may include:

- Identifying edge cases and abnormal scenarios
- Establishing intervention thresholds
- Defining human oversight parameters
- Demonstrating traceability between requirements and behaviour

Regulators have published guidance material addressing artificial intelligence and machine learning integration into aviation systems. The focus is not on accelerating automation, but on ensuring that assurance methodologies evolve alongside it.

In this environment, autonomy development is inseparable from autonomy governance.

Systems Integration as Risk Governance

Aircraft are no longer collections of largely independent subsystems. They operate as networked architectures in which data flows continuously between flight controls, avionics, sensors and communication systems.

Systems integration leads manage this interaction layer. Their responsibilities include:

- Defining communication hierarchies and data buses
- Controlling cross-system dependencies
- Preventing cascading or emergent failure modes
- Ensuring human-machine interfaces remain coherent under degraded conditions

As digital architectures become more complex, integration risk increases. Seemingly isolated software changes may influence unrelated functions if not properly partitioned.

Risk management therefore depends on disciplined architectural governance rather than isolated component reliability.

A Cultural Shift in Aviation Leadership

Historically, aviation authority was strongly associated with aerodynamic design, propulsion reliability and flight test evaluation. Those disciplines remain central.

However, the centre of gravity has shifted. Safety outcomes increasingly depend on:

- Logical partitioning
- Requirements integrity
- Configuration control
- Software update governance
- Validation independence

These responsibilities sit primarily with software architects and systems engineers.

The cockpit remains visible. The codebase remains largely unseen. Yet the latter now defines much of the former's behaviour.

Drones as Context, Not Centre

Uncrewed systems illustrate this shift clearly, as behavioural authority rests entirely in software logic. However, the trend is not confined to remotely piloted or autonomous aircraft.

Transport category aircraft, business jets and regional platforms increasingly rely on integrated digital architectures. The same standards, safety cases and assurance disciplines apply.

The structural lesson extends beyond any single platform type: as aircraft become software-defined systems, the individuals responsible for code architecture become central figures in aviation safety.

The evolution of aviation has always been shaped by engineering leadership. Today, that leadership is increasingly exercised through software architecture, assurance frameworks and systems integration discipline.

The professionals defining aircraft behaviour may not occupy the flight deck or the test range. They operate within development environments, safety assessment reviews and certification discussions.
Yet their influence is profound.

The quiet rise of aviation software architects signals a structural change in how safety authority is exercised. In the software-defined era, the control column is no longer the sole symbol of command. Architecture has become the new locus of aviation governance.

DESIGNING FOR AUTONOMY: AUTOMATION AS SYSTEM ARCHITECTURE

Robotics, software stacks and the hidden fragility inside aerospace production.

Automation is no longer a future upgrade in aerospace manufacturing. It is structural. But when production becomes software-defined, resilience depends less on mechanical throughput and more on the integrity of data, integration and digital supply chains.

The Software-Defined Factory

Across aerospace production floors, automation is no longer framed as an experiment in efficiency. It is increasingly presented as a response to two converging pressures: a shrinking skilled workforce and the need to maintain uncompromising quality at higher production rates.

Robotic drilling, automated fibre placement, additive manufacturing and digitally controlled inspection systems are being deployed not because they are novel, but because the human capacity to scale production is constrained.

Manufacturers such as Airbus are exploring expanded use of robotics to stabilise quality and reduce rework in environments defined by tight tolerances and long qualification cycles.

In this context, automation is less about replacing people and more about ensuring continuity of output. But continuity in a software-driven factory depends on more than mechanical reliability.

When Bottlenecks Move Upstream

Automation reduces reliance on scarce labour. It does not eliminate dependency — it relocates it.

An automated production line depends on robotics hardware, controllers, sensors, specialised software, vendor support and integration engineering aligned with traceability requirements.

Industry work on supply chain resilience highlights how capacity, visibility and collaboration shape manufacturing continuity.

In a highly automated environment, those dependencies deepen. Production becomes sensitive to suppliers whose failure modes are less visible than traditional component shortages.

In a software-defined factory, disruption may originate in a controller firmware update, an unavailable integrator, or a compromised operational technology environment — not only in a missing fastener.

Automation removes one bottleneck. It may expose another.

Precision As Risk Management

Aerospace manufacturing has always relied on highly skilled labour trained over years. That workforce is ageing, while competition from other advanced manufacturing sectors intensifies.

Robots apply torque consistently, lay composite fibres with micron-level precision and repeat tasks without drift.

In a regulated industry where conformity underpins safety and certification, precision is not merely an efficiency metric. It is a risk-control mechanism.

The shift toward automation therefore reflects more than labour economics. It represents a structural move towards production systems in which software logic increasingly governs quality outcomes.

Cybersecurity As A Production Variable

As industrial robots and automated machining systems connect to enterprise IT for monitoring and analytics, the attack surface expands.

Guidance from institutions such as the National Institute of Standards and Technology and the Cybersecurity and Infrastructure Security Agency exists because industrial environments are high-value targets.

In aerospace manufacturing, a cyber incident does more than interrupt output. It can compromise traceability, data integrity and quality assurance records, triggering extensive recovery and revalidation.

When production becomes data-driven, trust in production data becomes as critical as the integrity of the physical structure being built.

A Supply Chain That Now Includes Code

The Aerospace Industries Association notes that modern supply chains involve hardware, software and data flowing across multiple organisations.

Standards such as the ISA/IEC 62443 series reflect the need for lifecycle management of operational technology security.

As manufacturers integrate advanced analytics for predictive maintenance, machine-vision inspection and optimisation, complexity increases further.

Adding intelligence enhances defect detection and output stability. But it also introduces governance and security obligations that must be deliberately managed.

In a software-defined manufacturing ecosystem, resilience is no longer purely mechanical. It is architectural.

Why This Matters Beyond The Factory

Manufacturing fragility does not remain confined to production floors. When output slows or parts availability falters, airlines absorb the impact through delayed deliveries, spares scarcity and maintenance disruption.

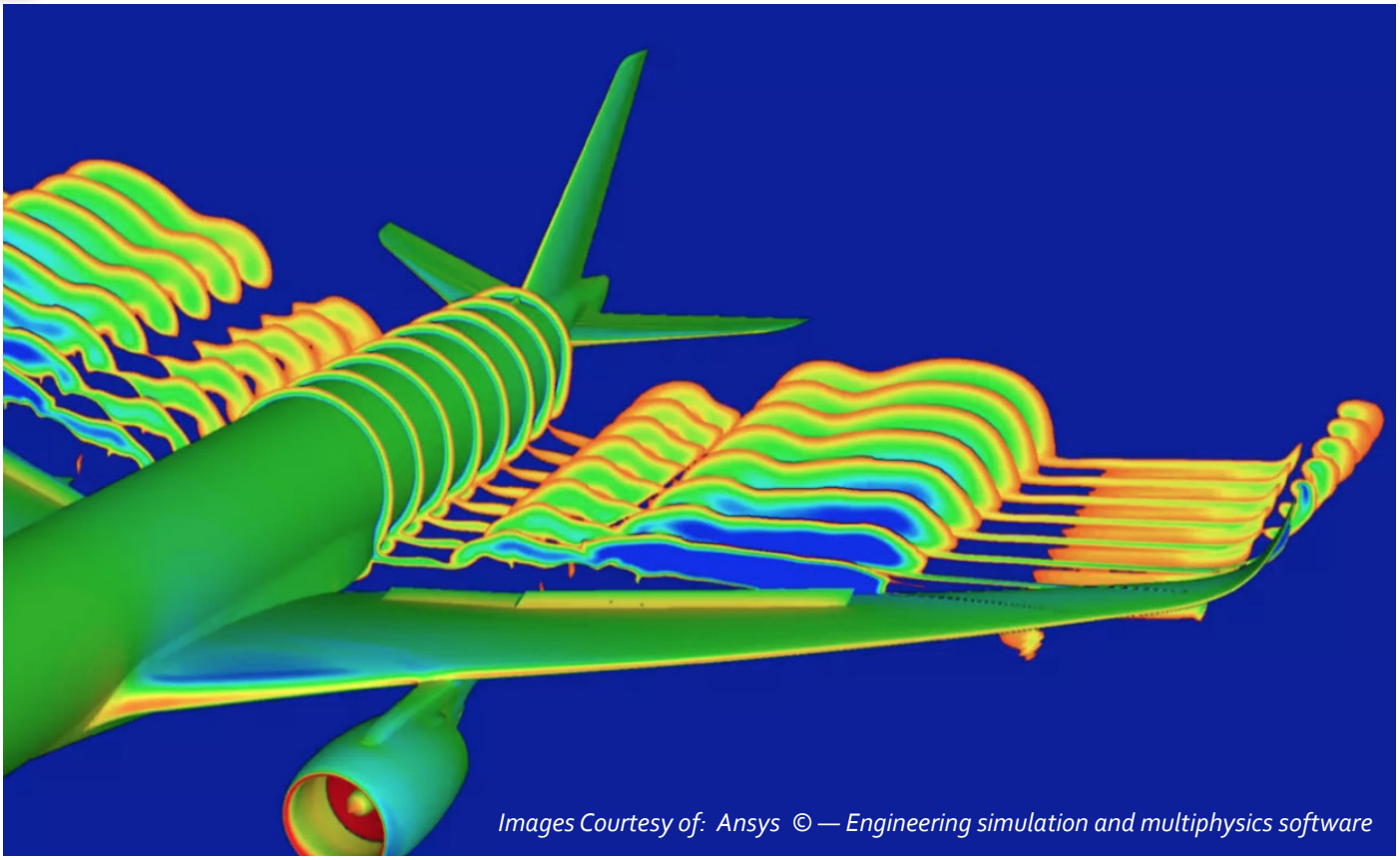
Automation can stabilise output. It cannot guarantee resilience if upstream digital dependencies remain fragile.

Automation As A System, Not A Cure

Automation will remain central to aerospace production ramp-ups. It improves consistency, addresses labour constraints and supports higher output rates.

But in a software-defined manufacturing environment, success depends on more than robotics. It requires robust integration engineering, secure operational technology networks and deliberate management of digital supply chains.

The strategic question is not whether to automate. It is whether automation is being deployed with resilience in mind. As aviation transitions from hardware-led systems to software-defined architecture, intelligence increasingly governs not only how aircraft fly — but how they are built.



Images Courtesy of: Ansys © — Engineering simulation and multiphysics software

PREDICTING FAILURE BEFORE FLIGHT: HOW ANSYS SHAPES MODERN AIRCRAFT DESIGN

The first structural test of a modern aircraft no longer begins on a runway or in a laboratory hangar. It begins in a simulation environment.
Before metal is cut, composites are laid or engines are run, engineers model how components will bend, vibrate, heat, fatigue and potentially fail. In contemporary aerospace programmes, predictive simulation is not an adjunct to engineering. It is embedded in the design process.

Ansys is one of the companies whose software tools underpin that shift.

From Prototype to Predictive Model

Ansys develops engineering simulation software used across aerospace for structural analysis, computational fluid dynamics, electromagnetics and thermal modelling.

Historically, aircraft development relied heavily on iterative physical prototyping and destructive testing to reveal structural weaknesses. While physical validation remains mandatory for certification, simulation now enables engineers to identify stress concentrations and failure risks earlier in the design cycle.

Using finite element analysis (FEA), engineers can simulate how airframe components respond to load conditions, vibration patterns and fatigue cycles. Computational fluid dynamics (CFD) tools model airflow behaviour across wings, nacelles and control surfaces, supporting aerodynamic optimisation and icing analysis.

The result is not the elimination of physical testing. It is the narrowing of uncertainty before physical hardware is produced.

Modelling Failure Before It Occurs

In aerospace applications, Ansys software is used to:

- Predict crack initiation and propagation
- Analyse load distribution across composite structures
- Simulate vibration-induced fatigue
- Model lightning strike effects and electromagnetic interference
- Assess thermal behaviour in engines and avionics systems

Modern aircraft incorporate lightweight composite materials, densely integrated avionics and, increasingly, electric propulsion components. These introduce new structural and thermal interactions.

Multiphysics simulation — modelling interactions between mechanical, thermal and electromagnetic domains — allows engineers to assess how stresses in one system may influence performance in another.

This approach reduces the likelihood of emergent failures that only become apparent during late-stage testing.

Simulation in the Certification Context

Regulatory authorities such as the Federal Aviation Administration and the European Union Aviation Safety Agency continue to require physical validation and formal compliance documentation.

However, simulation results are widely used to:

- Support structural substantiation reports
- Inform safety assessments
- Demonstrate compliance margins
- Define parameters for physical test campaigns

In many aerospace programmes, digital modelling informs where and how physical tests are conducted.

Model-based engineering frameworks integrate requirements, design architecture and verification artefacts, creating traceable links between simulated performance and documented compliance evidence.

Simulation does not replace certification testing. It shapes the path toward it.

Beyond Design: Lifecycle and Digital Twins

Simulation tools are increasingly connected to operational data streams through digital twin methodologies.

By linking design models with in-service sensor data, operators and manufacturers can:

- Monitor component stress exposure
- Predict degradation patterns
- Adjust maintenance intervals
- Anticipate potential failure modes

This lifecycle application extends predictive modelling beyond initial design into fleet operations.
The aircraft component exists not only as a physical asset, but as a continuously updated digital representation reflecting operational history.

A Structural Layer in Software-Defined Aviation

The shift toward software-defined aviation is often associated with autonomy and avionics. Engineering simulation represents an earlier layer of that transformation.

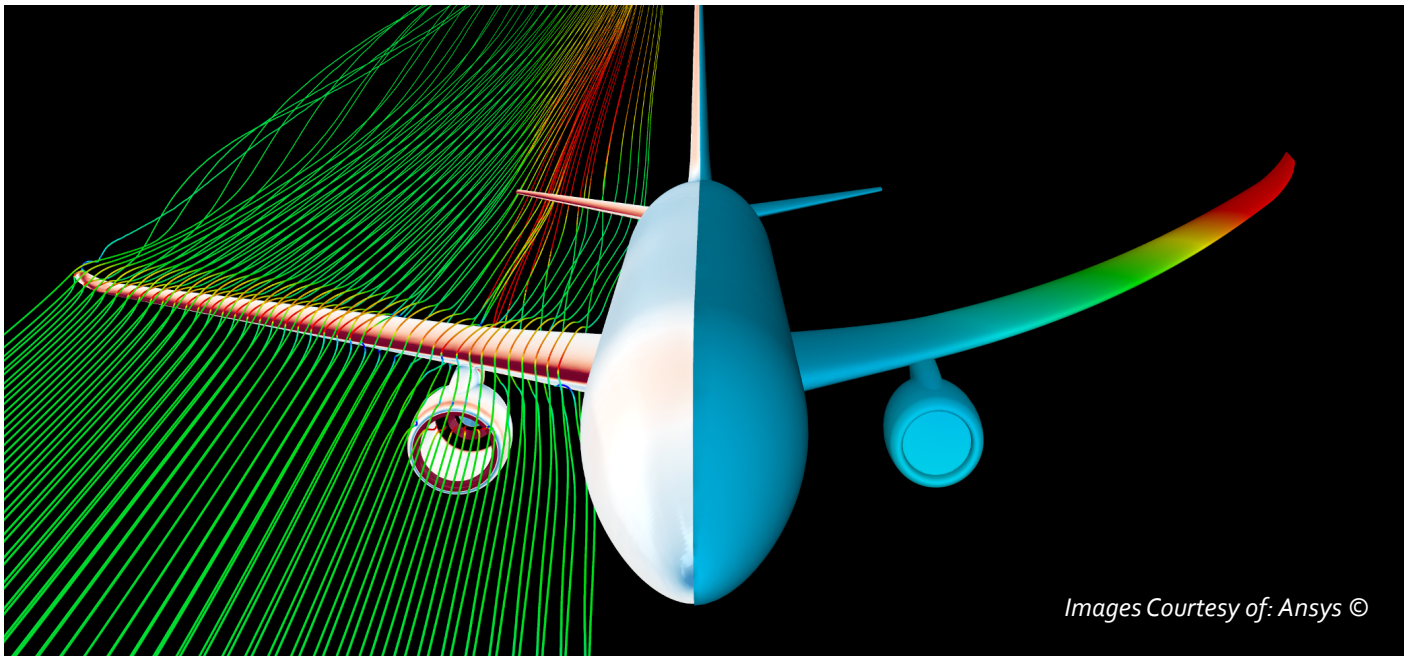
Before flight control logic is certified and before operational software governs performance, structural margins and system tolerances are defined in predictive modelling environments.

In this context, the first identification of potential failure often occurs in code rather than in metal.

Engineering authority increasingly resides in digital analysis environments that inform material selection, structural reinforcement and safety margins before physical validation begins.

Aircraft remain physical machines governed by aerodynamic principles and structural limits. However, the determination of those limits increasingly begins in simulation environments.

Companies such as Ansys provide the tools that allow engineers to predict behaviour under stress before components are manufactured or assembled.
In modern aerospace programmes, the first flight may still occur on a runway. The first structural test, however, often occurs in a virtual model.



Images Courtesy of: Ansys ©

THE NEW LOGIC INSIDE MODERN AIRCRAFT

Airbus and Singapore demonstrate crewed–uncrewed integration in live flight trials.

Modern air power is no longer defined solely by the performance of a single aircraft. Increasingly, capability is determined by how platforms connect, share data and coordinate in real time. Airbus and Singapore's recent HTeaming flight trials illustrate this shift, demonstrating how software architecture can link crewed and uncrewed aircraft into a single operational system.

From Platform To Network

Airbus and Singapore's Defence Science and Technology Agency (DSTA) have successfully completed a crewed–uncrewed flight demonstration at a Singapore airbase. The January trials marked the first integration of Airbus' HTeaming system between a Republic of Singapore Air Force (RSAF) H225M helicopter and an Airbus Flexrotor uncrewed aerial system (UAS).

Under an agreement signed in June last year, the partners explored how such integration could enhance

Images Courtesy of: Airbus

Airbus Flexrotor. Images Courtesy of Airbus

situational awareness and mission outcomes through coordinated operations.

In simulated search-and-rescue scenarios, the H225M crew accessed real-time data from the Flexrotor, extending visual range and improving mission safety. Crucially, the helicopter crew maintained direct command and control of the UAS while receiving live operational data.

The demonstration was not simply about operating two aircraft together. It was about connecting them through a shared data environment.

Data-Link Architecture As Mission Enabler

Airbus managed the design of the HTeaming system and its integration into the H225M, including specialised data-link architectures.

This architecture enabled the helicopter crew to receive, process and act on real-time data from the Flexrotor while retaining operational authority. The integration facilitated rapid decision-making and reduced exposure to high-risk environments.

Rather than adding another platform into the airspace, the system created a distributed operational picture. The helicopter effectively became a command node within a wider networked mission structure.

Human Decision-Making Remains Central

DSTA emphasised that the capability enhances mission effectiveness while ensuring human decision-making remains at the centre of operations.

As aviation systems grow increasingly interconnected, clarity of command authority becomes critical. Crewed–uncrewed teaming does not remove the pilot from the loop. It extends the pilot's reach through integrated sensors, secure data-links and coordinated control logic.

In this environment, autonomy supports — rather than replaces — human oversight.

Modular And Uas-Agnostic Design

Airbus describes HTeaming as a modular, UAS-agnostic solution compatible across its helicopter range. The system is designed to integrate multiple uncrewed platforms, allowing crews to assume control of different UAS in flight depending on mission requirements.

The Flexrotor, a 25 kg vertical take-off and landing uncrewed aircraft, is designed for extended ISTAR missions and can autonomously launch and recover within a compact footprint. Its integration with the H225M illustrates how lightweight autonomous systems can expand the operational envelope of larger crewed platforms.

Networked Operations As Structural Shift

The H225M, part of the Super Puma family, is recognised for performance in demanding environments. Through HTeaming integration, its capability extends beyond range and payload into networked coordination.

This development reflects a broader structural change across aerospace systems.

Aircraft are no longer defined solely by mechanical performance. They are increasingly defined by the software architectures that connect them.

The airframe remains visible. But operational authority increasingly resides in the code that links platforms together.

CERTIFYING CHANGE: OVERSIGHT IN THE SOFTWARE-DEFINED ERA

An aircraft enters service under a certified configuration. Its systems, software and structural margins have been validated against defined requirements. The type certificate is granted. Airworthiness is established.

In the early decades of powered flight, certification focussed on static artefacts — the physical airframe, fixed mechanical systems and discrete functions, tested until the system could be verified against a defined configuration baseline.

Six months later, a software update is introduced. A cybersecurity mitigation is added. A performance optimisation is implemented. A digital model is refined. Is it still the same aircraft?

In a software-defined era, certification is no longer solely a fixed event at entry into service. It is supported by continuing oversight throughout the aircraft lifecycle. Modern aircraft rely on software that governs flight control laws, navigation, engine management, displays and increasingly autonomous capability.

From Frozen Configuration To Managed Evolution

Traditional certification assumed relative physical stability. Hardware was fixed, tested and approved. Changes required classification and approval through established mechanisms such as amended type certificates, supplemental type certificates or approved design organisation processes. Airworthiness was preserved through inspection, maintenance and configuration control.

The frozen configuration provided a defined compliance baseline against which changes could be assessed. Software alters that operational reality.

Modern aircraft contain millions of lines of code across avionics, flight control logic, health monitoring and communications. Navigation databases are routinely updated. Cybersecurity protections evolve. Digital tools interact directly with certified hardware and systems.

Regulators must therefore approve not only aircraft at entry into service, but also the organisational and engineering processes that govern subsequent change. Certification increasingly emphasises the approval and oversight of those change-management processes, alongside continued product-level compliance.

EASA: Regulator As System Actor

The European Union Aviation Safety Agency has adopted a structured response to adaptive and learning-enabled technologies through its Artificial Intelligence Roadmap[2] and related Concept Papers[3]. The Federal Aviation Administration has likewise placed increasing emphasis on process-based oversight within established certification frameworks.

EASA's AI Roadmap recognises that adaptive systems require defined operational design domains, monitoring frameworks and clear human oversight. Its information security regulation, Part-IS[1], embeds cybersecurity risk management obligations within the regulatory architecture for aviation organisations.
Regulatory oversight now places particular emphasis on:

- Traceable software change management
- Continuous safety and risk assessment
- Integration of cybersecurity within safety systems
- Proper documentation of digital and model-based evidence

In this environment, the regulator becomes an active participant in ensuring that technical evolution remains controlled and compliant.

Faa: Approving The Process, Not Just The Product

The Federal Aviation Administration faces similar structural adjustments. Oversight increasingly examines how software is developed, maintained and updated within approved design and safety frameworks.

Standards such as DO-178C[4], formally recognised by the FAA through Advisory Circular AC 20-115D[5], remain central to airborne software certification. Continued operational safety processes place greater emphasis on how post-certification changes are classified, managed and verified.

Regulatory scrutiny includes configuration control, software revision traceability, Safety Management System integration[6], cybersecurity governance frameworks[7] and operational data monitoring.
Rather than treating every software revision as a full re-certification event, authorities assess whether changes are appropriately classified and managed within approved design organisation and oversight structures.
The emphasis shifts from static approval toward controlled and traceable evolution.

Third-Party Assurance: Expanding The Ecosystem

As systems grow more complex, independent assurance bodies assume a larger complementary role.

Traditional airworthiness frameworks primarily addressed unintentional system failures rather than adversarial cyber threats. In recent years, cybersecurity has become an increasingly formalised component of safety and risk management, including through standards such as DO-326A[7].

Organisations such as DNV provide risk-based auditing and digital risk certification across critical infrastructure sectors. TÜV SÜD contributes functional safety and cyber-physical validation expertise relevant to aerospace environments.

Certification authority remains with regulators, but assurance activities increasingly draw on broader risk governance capability across interconnected technical domains.

The Certification Challenge of Adaptive Systems

Adaptive systems present a core challenge. Process approval does not replace product assessment — it supports it. Regulators evaluate disciplined engineering processes capable of managing change safely over time, while retaining authority over significant design changes.

When algorithms are refined or cybersecurity measures updated, future system states must remain bounded within validated operational limits. Monitoring mechanisms, fallback modes and documented update governance procedures become central safeguards.

The objective is not to constrain innovation, but to ensure that system evolution remains predictable, traceable and compliant with the certification basis.

Digital Evidence and Model-Based Oversight

Digital twins and model-based systems engineering introduce further complexity.

Simulation environments now generate evidence used to support safety cases and compliance documentation. Regulators must assess not only physical testing results, but also the validity, traceability and configuration control of digital models used in certification artefacts.

Oversight extends to verification traceability, model validation methodology and integration of simulation outputs into approved compliance frameworks.

Certification authority is expanding from inspection of hardware to structured review of system logic, digital evidence and engineering governance processes.

Aviation remains one of the world's most rigorously regulated industries. That discipline is not diminishing. It is adapting to technological evolution.
Certification is no longer confined to approving a machine at a single point in time. It now encompasses ensuring that the mechanisms governing change remain robust, traceable and compliant throughout the aircraft lifecycle.
The frozen configuration provided certainty in a comparatively static technological environment. In a future defined by software, connectivity and rapid iteration, certification frameworks must support managed evolution without diluting safety assurance.
In the software-defined era, certifying change is as important as certifying design.

References
[1] *Commission Implementing Regulation (EU) 2022/1645 – Information Security (Part-IS), Official Journal of the European Union, 2022.*
[2] *European Union Aviation Safety Agency (EASA), Artificial Intelligence Roadmap 2.0: A Human-Centric Approach to AI in Aviation, 2023.*
[3] *EASA, Concept Paper: First Usable Guidance for Level 1 Machine Learning Applications, 2021.*
[4] *RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, RTCA, Inc., 2011.*
[5] *FAA Advisory Circular AC 20-115D, Airborne Software Development Assurance Using RTCA DO-178C, Federal Aviation Administration, 2017.*
[6] *FAA Advisory Circular AC 119-1, Safety Management Systems for Air Carriers, Federal Aviation Administration.*
[7] *RTCA DO-326A / EUROCAE ED-202A, Airworthiness Security Process Specification, 2014.*

Getting you there

- Safely
- Reliably
- Comfortably
- Cost Effectively

Training

AIR-TEC has the only appro
FNPT 2 Simulator in the So
Hemisphere.

AOCs

- SACAA South Africa
- DCA Mauritius
- IACM Mozambique

sales@air-tecm.com | www.air-tecm.com

29	L410 / L420
11	B1900D
1	B200
1	BELL 206

oved L410 –
uthern

Our Core Business

- Aircraft Leasing ACMI
- Aircraft Sales
- Aircraft Maintenance, Factory Service Centres
- Pilot & Engineer Training
- Aircraft Management

AIR-TEC GLOBAL

BARS BASIC AVIATION RISK STANDARD GOLD FLIGHT SAFETY FOUNDATION


©WAN

DIGITAL TWINS: WHEN AVIATION TESTS REALITY BEFORE METAL EXISTS

As autonomy increases, simulation becomes part of the safety architecture.

Aviation has always relied on testing before entry into service. Wind tunnels, structural rigs and flight trials established confidence before aircraft carried passengers. Today, an additional proving ground is taking shape: high-fidelity digital twins. As aircraft systems become increasingly software-defined — and as autonomy expands — simulation is no longer only a design convenience. It is becoming part of the safety architecture itself.

From Design Tool To Safety Infrastructure

The concept of a digital twin is rooted in numerical simulation and model-based engineering. In aviation terms, it represents a virtual environment capable of reproducing aircraft, operational systems or airspace behaviour under defined conditions.

Research literature reviewed by EASA highlights digital twins as an evolution of advanced simulation frameworks, enabling analysis across a system's lifecycle rather than solely at the point of design. In parallel, NASA has advanced work on a National Airspace System (NAS) Digital Twin — a realistic simulation environment capable of modelling current and future airspace operations before changes are introduced into live traffic environments.

This represents a structural shift. Simulation is no longer confined to performance prediction. It is increasingly used to evaluate operational interaction, system integration and risk exposure.

The Drone Domain: Where Simulation Becomes Essential

Uncrewed aircraft systems (UAS) provide the clearest demonstration of why digital twins are becoming central.

In most drones, flight stability, navigation, obstacle avoidance and contingency behaviour are governed by software logic from inception. Unlike traditional mechanically mediated aircraft, UAS platforms rely almost entirely on sensor fusion, computational interpretation and algorithmic response.

As autonomy increases, testing cannot rely solely on physical flight hours. Certain edge cases — rare weather conditions, unusual visual surfaces, degraded communication environments — cannot be safely or economically reproduced repeatedly in the real world.

Digital twin environments therefore serve several critical roles:

- Mission rehearsal environments, allowing operators and regulators to evaluate operational concepts without exposing live airspace to unproven risk. Airbus UTM's USim platform, for example, provides a digital twin of the UTM ecosystem to test interoperability and services before operational deployment.
- Sensor validation under variable environmental conditions, enabling examination of how perception systems respond to low contrast, haze, dust or complex urban geometries. The credibility of autonomy depends on how accurately these variables are represented in simulation.
- Swarm and high-density modelling, where multiple UAS interact within constrained airspace. Emergent behaviour in coordinated systems cannot be evaluated solely through isolated test flights.

Research into digital twin corridors and hybrid flight environments — combining real aircraft with simulated traffic — demonstrates how autonomy concepts are stress-tested before scaling.

In this domain, simulation is not aspirational. It is precautionary.

Bridging To Certification

Digital twins do not replace certification. They reshape its evidentiary base.

Airborne software remains subject to structured assurance frameworks, with regulators requiring documented validation, verification and impact analysis for changes. The FAA's advisory guidance on software change impact analysis underscores that behaviour defined in code must be traceable and assessed whenever modifications occur.

As aircraft behaviour becomes increasingly software-mediated, certification authorities must determine how simulation evidence is validated. Analogy can be drawn to flight simulation training devices (FSTDs), where qualification depends on validated source data demonstrating that the simulator faithfully represents the aircraft.

The same principle applies to digital twins used in design or operational validation: the simulation must itself be demonstrably representative.

The more autonomy defines safety margins, the more regulators require confidence in the models used to assess those margins.

Airports And Airspace As Digital Systems

The digital twin concept extends beyond individual aircraft.

Airport operators are increasingly deploying digital twin platforms to model passenger flow,

ground movement and operational resilience. ICAO documentation highlights the integration of digital tools to support proactive safety management and system optimisation.

Similarly, NASA's NAS Digital Twin initiative seeks to model the behaviour of the airspace system as a whole — evaluating integration of new entrants and emerging traffic concepts within a realistic computational environment before live implementation.

Airspace, like aircraft, is becoming software-defined. When traffic density increases and autonomy expands, modelling becomes a prerequisite for safe integration.

Realism As A Safety Requirement

Simulation has always involved abstraction. Digital twins raise the standard.

If autonomy logic depends on sensor fidelity, then environmental modelling must accurately reflect the conditions that challenge perception. If coordinated drone fleets operate in shared corridors, then latency, link degradation and communication failure must be represented realistically.

The more autonomous the aircraft, the more real the simulation must become.

Without credible modelling, digital twins risk becoming design tools rather than safety instruments.

From Prototype To Governance

Digital twins are evolving from engineering aids to governance mechanisms.

They enable:

- Pre-deployment risk evaluation
- Scenario stress-testing
- Integration assessment for new entrants
- Data-informed operational planning

Yet they also introduce new responsibilities. Models must be updated, validated and governed as operational conditions evolve. Simulation integrity becomes part of lifecycle oversight.

In a software-defined aviation ecosystem, assurance does not stop at hardware inspection. It extends to the credibility of the environments in which systems are tested.

When Reality Is Tested Twice

Aviation has never relied on a single layer of safety. Physical testing remains indispensable. Flight trials remain definitive. But as systems grow more autonomous and interconnected, digital twins provide a second proving ground — one capable of exposing interaction effects before they manifest in live operations.

Aircraft are no longer assessed only in wind tunnels and on runways. They are evaluated in models, networks and simulated airspace ecosystems.

In the software-defined sky, reality is tested twice — once in code, and once in flight.

THE LARGEST GATHERING OF DECISION MAKERS AND BUYERS ON THE AFRICAN CONTINENT

25 AFRICA AEROSPACE & DEFENCE 16-20 SEPT 2026

16 - 20 SEPT

#AAD2026

YOUR GATEWAY TO CUTTING-EDGE TECHNOLOGIES IN GLOBAL DEFENCE AND AEROSPACE

BOOK YOUR SPOT NOW!

WWW.AADEXPO.CO.ZA | AIR FORCE BASE WATERKLOOF, CITY OF TSHWANE

PARTNERS: AMD SOUTH AFRICAN, ARMSCOR, CAASA, defence Department REPUBLIC OF SOUTH AFRICA

SUPPORTED BY: the dtic Department Trade, Industry and Competition REPUBLIC OF SOUTH AFRICA

HOST CITY: CITY OF TSHWANE

CYBER + SAFETY:– WHEN RESILIENCE MATTERS MORE THAN SPEED

As drones transition from standalone aircraft to networked aviation systems, their dominant risk profile changes. Mechanical failure remains a traditional safety concern. Software compromise, signal interference and data manipulation introduce a different class of risk — one that can scale rapidly, propagate across fleets and challenge established airworthiness assumptions. In this environment, resilience increasingly matters more than speed.

Software Failure Is Not Mechanical Failure

Conventional aviation safety evolved around physical components: engines, structures, hydraulics and flight controls. Failure modes were observable, inspectable and often contained to a single aircraft.

Drone systems operate differently. They are software-defined, network-dependent and frequently reliant on satellite navigation and command links. A defect in code, a corrupted configuration or an exploited communication pathway does not remain local. It may affect multiple aircraft simultaneously, particularly where fleet management platforms and shared update systems are used.

Airworthiness security frameworks developed by RTCA and EUROCAE, including DO-326A / ED-202A, explicitly recognise that cybersecurity is not an IT matter but a direct safety consideration. When aircraft behaviour is determined by software logic, system integrity becomes inseparable from operational safety.

Expanding Attack Surface

The modern drone is effectively a connected node within a broader digital ecosystem. Its attack surface extends beyond the airframe to include:

- Satellite navigation inputs
- Command-and-control (C2) links
- Ground control systems
- Cloud-based fleet management platforms
- Over-the-air software update pipelines
- Artificial intelligence decision models

Each connection introduces dependency. Each dependency introduces exposure.

International civil aviation bodies are now treating interference and cyber vulnerability as operational realities rather than theoretical concerns. ICAO has published material addressing GNSS vulnerabilities and mitigation strategies. EASA and IATA have similarly outlined coordinated responses to increasing GNSS interference events affecting civil aviation operations.

Drone-Relevant Risk Types

- **GNSS spoofing**: Global Navigation Satellite Systems underpin most drone navigation architectures. Spoofing involves broadcasting counterfeit signals that cause the aircraft to calculate an incorrect position or velocity solution.

  For a drone, this may result in diversion, airspace infringement, loss of containment or impact with terrain or infrastructure. Unlike mechanical faults, spoofing manipulates the aircraft's perception of reality.

  Regulators including ICAO, EASA and the FAA have acknowledged increasing reports of GNSS interference affecting civil operations, reinforcing the need for cross-checking, integrity monitoring and degraded-mode procedures.
- **Command-link interruption**: The C2 link enables pilot authority or supervisory oversight. Interruption — whether through jamming, interference or network disruption — can trigger lost-link behaviours.

  Safe recovery depends on pre-programmed contingencies. In complex airspace or urban environments, these contingencies may not always align with dynamic operational risk. Resilience therefore requires more than maintaining link strength; it demands predictable, safety-assured behaviour under link degradation.
- **Data corruption**: Corrupted navigation databases, altered geofencing parameters, compromised telemetry or manipulated configuration settings may not immediately appear as system failure. Instead, they bias decision-making and situational awareness.

  The FAA has examined UAS fleet cybersecurity vulnerabilities, highlighting the importance of configuration management, secure defaults and integrity verification across entire fleets. In networked operations, data integrity becomes a primary safety control.
- **AI decision poisoning**: As drones increasingly incorporate autonomy features, machine learning models influence perception, object identification and route selection. Adversarial manipulation of training data or operational inputs — often referred to as AI poisoning — can distort decision logic without physically breaching the aircraft.

  NIST's work on adversarial machine learning underscores that AI assurance must include testing, monitoring and defined human intervention pathways.

  In aviation, decision reliability under adversarial conditions becomes a safety question rather than a performance metric.
- **Fleet-level systemic failure**: Perhaps the most significant distinction between mechanical and digital risk lies at fleet scale. A shared software vulnerability, flawed update deployment or common configuration weakness can affect multiple aircraft concurrently.

  This introduces the possibility of correlated failures — an aviation risk profile historically associated with systemic design flaws rather than operational anomalies.

  Drone fleets used for logistics, surveillance or inspection operate under centralised digital governance. The safety of each aircraft is therefore linked to the integrity of the broader digital architecture.

From Military Exposure To Civil Reality

Historically, aviation risk patterns migrate from military domains into civil and commercial environments as technology proliferates. GNSS interference, electronic warfare techniques and counter-drone capabilities have long been present in defence contexts.

As civil aviation increasingly depends on satellite

navigation, connectivity and software-defined systems, similar vulnerabilities manifest within commercial and airline operations.

The lesson is not alarmist. It is structural. Risk evolves alongside technology adoption. Civil frameworks must therefore adapt before disruption becomes systemic.

Resilience As An Operational Principle

Resilience in drone operations involves measurable engineering and governance practices:

- Multi-source navigation validation rather than sole reliance on GNSS
- Clearly defined and tested lost-link behaviours
- Secure configuration and update management
- Fleet-level cyber risk assessment
- AI assurance protocols with monitoring and intervention thresholds

Speed, autonomy and scalability remain commercial objectives. However, in safety-critical aviation contexts, the priority shifts toward predictable degradation and recoverability.

The defining safety question is no longer simply whether the aircraft flies correctly in nominal conditions. It is whether it remains controllable and trustworthy when its digital environment is disrupted.

Drones represent a decisive phase in aviation's software-defined transition. Their safety architecture depends less on mechanical robustness and increasingly on digital integrity.

When aircraft become network nodes, resilience becomes the governing discipline. In that context, safety is determined not by how efficiently systems operate when connected, but by how reliably they perform when connectivity, data or logic cannot be fully trusted.

How Airlines Are Preparing For Gnss Disruption

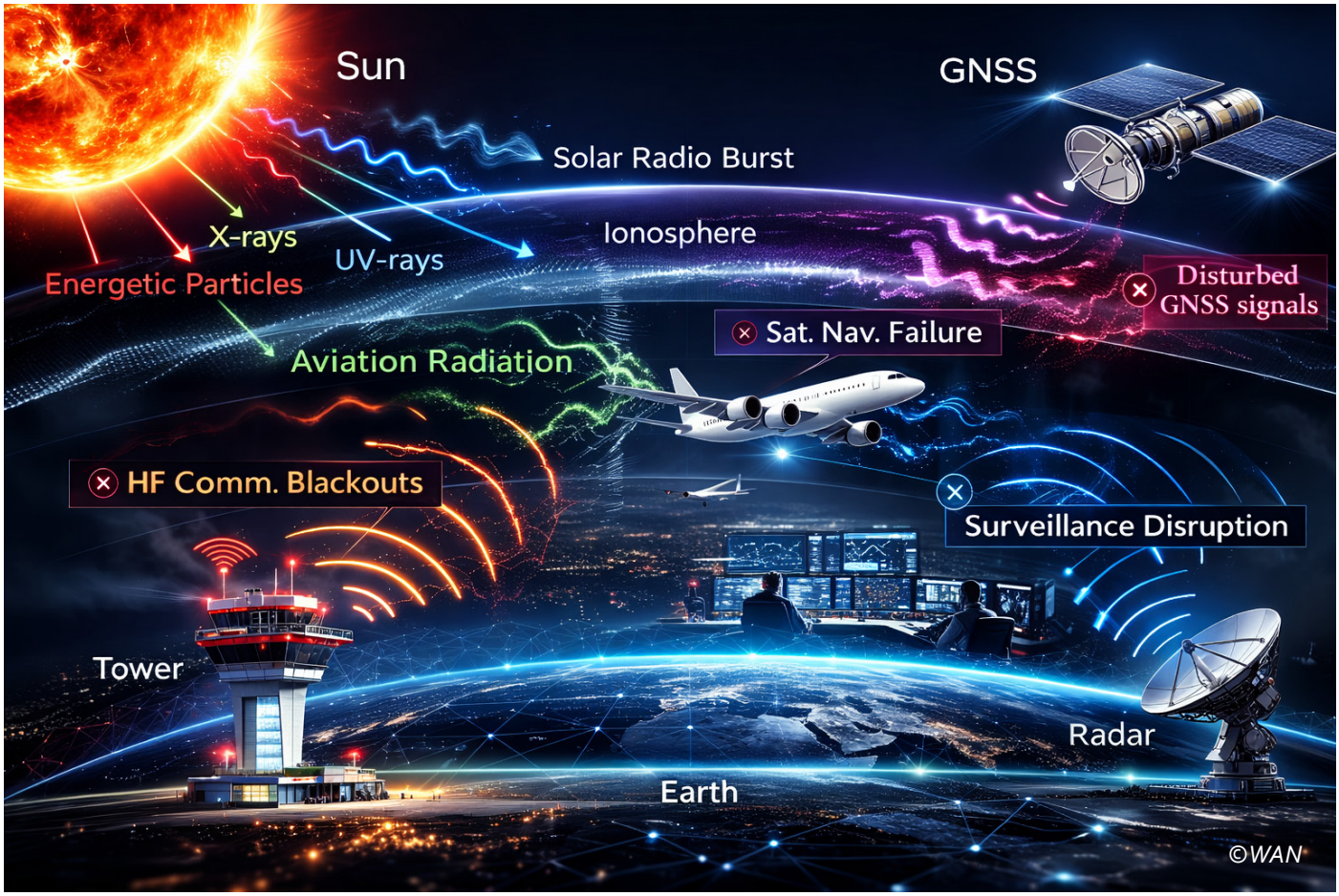
While drone operations highlight the cyber-safety dimension of satellite navigation dependency, airlines are confronting similar vulnerabilities within conventional transport operations.

Reports of GNSS interference — including jamming and spoofing — have increased in several regions, prompting coordinated responses from regulators, operators and industry bodies.

Procedural Resilience

Airlines continue to train crews for navigation degradation scenarios. Conventional radio navigation aids, inertial reference systems and cross-checking procedures remain integral components of flight operations.

Flight crews are trained to recognise GNSS anomalies, including unexpected position shifts, inconsistent ground speeds or discrepancies between independent navigation sources. In such cases, standard operating procedures prioritise cross-verification and reversion to alternative navigation methods.



Regulatory authorities, including the Federal Aviation Administration and the European Union Aviation Safety Agency, have issued operational guidance outlining crew awareness, reporting protocols and contingency procedures for GNSS interference environments.

Technical Mitigation

Modern transport aircraft are typically equipped with multi-sensor navigation architectures. GNSS inputs are integrated with inertial systems and, where available, ground-based navigation aids. This layered design reduces sole-source dependency.

Manufacturers and avionics suppliers are also developing enhanced integrity monitoring functions capable of detecting anomalous signal behaviour. Some operators have introduced additional software updates to improve alerting logic when GNSS reliability is compromised.

Airspace And Reporting Coordination

Airlines participate in structured reporting systems that allow interference events to be logged and analysed. Data shared with regulators supports the identification of geographic interference hotspots and informs risk assessments.

International coordination, including ICAO-led initiatives, seeks to standardise reporting terminology and mitigation strategies across states.

Operational Risk Management

From a governance perspective, GNSS disruption is now treated as an operational hazard requiring risk assessment, briefing and route planning considerations.

Airlines operating in regions with known interference patterns may adjust flight planning assumptions, review alternate aerodrome selections and reinforce crew briefings on navigation anomaly management.

The focus is not on eliminating satellite navigation dependency — which is now fundamental to modern aviation — but on ensuring that aircraft remain safely navigable when satellite integrity cannot be fully assured.

Bridging Drone And Airline Risk

The distinction between drone vulnerability and airline resilience is one of scale, not principle. Both rely on satellite navigation, software-defined avionics and integrated digital systems.

The drone environment illustrates how rapidly GNSS dependence can become a systemic exposure. Airline operations demonstrate how layered navigation architectures, procedural discipline and regulatory coordination provide mitigation.

In both domains, the safety objective is consistent: aircraft must remain controllable, navigable and predictable when digital inputs are uncertain.

REGULATOR GUIDANCE ON GNSS DISRUPTION

What regulators are recommending ICAO (Civil Aviation Authority)

- Recognises GNSS interference as a safety hazard.
- Calls for enhanced integrity monitoring, reporting and mitigation strategies across states.
- Recommends interoperability and data-sharing mechanisms to identify interference hotspots.

EASA (European Union Aviation Safety Agency)

- EASA (with IATA) has outlined a comprehensive plan to mitigate GNSS interference.
- Encourages states and operators to adopt procedural and technical mitigations for navigation outages.
- Promotes standardised reporting of GNSS anomalies across European airspace.

FAA (Federal Aviation Administration)

- Publishes a GPS/GNSS Interference Resource Guide for aviation stakeholders.
- Advises operators on spot reporting, monitoring procedures and redundancy of navigation sources.
- Identifies GNSS interference as an active safety concern, not a theoretical risk.

RTCA / EUROCAE

- Through the Airworthiness Security Process (DO-326A / ED-202A), embeds cybersecurity as a safety-critical requirement.
- Defines guidance on threat analysis, mitigation and software integrity requirements.
- NIST (National Institute of Standards and Technology)
- Provides an AI Risk Management Framework and adversarial ML taxonomy relevant to autonomous systems.
- Encourages rigorous assurance practices for systems that incorporate machine learning.

CYBERSECURITY AS SAFETY INFRASTRUCTURE

In a networked aviation environment, cyber disruption no longer affects data alone — it affects dispatch, airspace coordination and fleet continuity

An aircraft may be fuelled, crewed and technically serviceable. The weather may be within limits. The route may be cleared.

Yet if the digital systems supporting that aircraft are compromised, the flight does not depart.

Modern aviation depends on interconnected networks that extend well beyond the airframe. Dispatch systems, maintenance databases, airport operational platforms and air traffic management infrastructure form an integrated digital environment. When disruption occurs within that environment, the impact is measured not in data loss alone, but in delayed departures, reduced capacity and operational instability.

Cyber risk has moved from the background of aviation to its operational core.

From Network Event To Operational Disruption

Airlines rely on digital systems for crew allocation, aircraft routing, maintenance traceability and revenue management. Airports depend on networked platforms to coordinate baggage handling, gate management and airside operations. Air navigation service providers operate surveillance, flight data processing and communication systems that must remain continuously available.

These environments are increasingly interconnected. A cyber incident affecting one layer may have cascading consequences across others. Ransomware attacks and system intrusions in the transport sector have demonstrated that disruption can ground aircraft and interrupt passenger flows even when the aircraft themselves remain mechanically sound.

In this context, cyber resilience is inseparable from operational resilience.

Detecting The Abnormal

Cybersecurity approaches in aviation are evolving from perimeter defence to continuous monitoring.

Companies such as Darktrace apply behavioural anomaly detection to transport and critical infrastructure environments. By learning patterns of normal network behaviour, such systems can identify irregular activity that may signal compromise.

Within aviation, monitoring may extend across:

- Airport operational technology networks
- Airline enterprise systems
- Maintenance and compliance databases
- Communication infrastructures

The objective is not technological novelty. It is early intervention — identifying abnormal digital behaviour before it develops into operational paralysis.

In a networked aviation ecosystem, visibility is a prerequisite for continuity.

Where Digital And Physical Systems Converge

Cyber risk in aviation does not stop at enterprise networks. It intersects directly with operational platforms.

Leonardo develops integrated cyber-physical systems across aerospace and air traffic management environments. In these systems, software governs surveillance integration, mission management and command-and-control functions.

As aviation systems become more integrated, failure modes expand beyond mechanical breakdown. Disruption may arise from corrupted data flows, misaligned system logic or degraded communication pathways.

Mechanical integrity remains essential. Increasingly, so does software integrity.

The aircraft is physical. The system sustaining it is digital.

Resilience as Operational Discipline

Regulatory bodies recognise that digital system integrity is linked to safety and continuity. ICAO has issued aviation cybersecurity strategies, and European frameworks continue to strengthen information security oversight.

The emphasis is shifting from prevention alone to resilience.

In practical terms, this includes:

- Continuous network monitoring
- Segmentation of operational and enterprise systems
- Redundant communication pathways
- Structured response and recovery protocols

Absolute protection in complex networks is unrealistic. Operational stability depends on the ability to detect, contain and recover from disruption without halting flight operations.

This edition has examined software-defined aircraft, digital twins and computed airspace. Each reflects aviation's deepening reliance on digital architecture. That reliance introduces exposure.

When cyber risk becomes operational risk, resilience becomes a core aviation discipline. Innovation may shape the future of flight. Stability determines whether flight continues.

In a software-defined aviation system, cybersecurity is no longer a technical afterthought. It is part of the operational foundation that keeps aircraft moving and airspace stable.

Aviation Cyber Incidents — A Track Record Of Operational Disruption

Recent cyber events illustrate that digital disruption in aviation extends beyond theory. They show how attacks on supporting systems — not aircraft hardware — can ripple through operations:

Europe-wide airport service disruption (Sept 2025)

A ransomware attack against the vMUSE check-in and boarding platform operated by Collins Aerospace caused widespread delays and manual processing at major European hubs including London Heathrow, Berlin Brandenburg and Brussels Airport. Some airlines resorted to backup systems, while baggage handling and boarding delays persisted over several days.

Qantas customer data breach (Jul 2025)

Australia's flag carrier confirmed a cyber-attack on a third-party contact centre platform that exposed the personal records of up to six million customers. Systems were quickly secured, and authorities notified, but the incident highlighted the scope of risk associated with external vendors and shared digital services.

Hawaiian Airlines IT disruption (Jun 2025)

Hawaiian Airlines reported a cybersecurity incident that disrupted some IT systems. While flight operations continued normally and no safety impact was reported, the episode underscored how network compromise can affect airline operations even when mechanical systems remain unaffected.

Surging Cyber Activity Across Aviation Networks

Industry observers have noted a sharp increase in cyberattacks against the sector, with ransomware incidents rising by 600% between 2024 and 2025. These attacks target both operational and passenger-facing systems, amplifying pressure on airlines, airports and their suppliers to boost resilience.

Image Courtesy of: Dassault

FALCON 10X: BUSINESS AVIATION'S SOFTWARE-FIRST CERTIFICATION REALITY

While advanced air mobility platforms are often described as "born digital", the same certification reality already defines the top tier of business aviation. Dassault's Falcon 10X demonstrates how integrated avionics, fly-by-wire architecture and computing-driven flight decks are reshaping airworthiness from a predominantly structural exercise into a disciplined software and systems endeavour.

On specification alone, the Falcon 10X sits firmly at the pinnacle of long-range business aviation. Dassault publishes a range of 7,500 nautical miles (13,890 km) at Mach 0.85 (NBAA IFR reserves), a maximum Mach operating speed of 0.925, and a maximum certified altitude of 51,000 ft. Power is provided by two Rolls-Royce Pearl 10X engines, each rated at over 18,000 lb of thrust.

Cabin dimensions are equally notable, with Dassault stating approximately 2.03 m in height, 2.77 m in width and 16.4 m in length (excluding the flight deck and baggage compartment), positioning the aircraft at the top end of the ultra-long-range category.

The age of predominantly mechanical flight decks and isolated avionics has given way to 'born-digital' aircraft — platforms conceived from the outset as integrated, computer-driven systems. Nowhere is this transformation clearer than in the design and development of the Falcon 10X business jet, a platform that illustrates how modern airworthiness is evolving from a structural exercise into a disciplined software and systems endeavour.

Yet the more consequential story for certification lies not in range or cabin volume, but in architecture.

The Falcon 10X next-generation cockpit will feature Dassault's NeXus flight deck, built around the Honeywell Primus Epic integrated avionics platform.

This environment replaces federated avionics units with a computing-centred system built on large-format displays, centralised processing and software-driven functionality. The NeXus flight deck — which recently won the prestigious Good Design® Award — integrates high-resolution touchscreen interfaces, automated

systems, and advanced visualisation in a cohesive digital environment that reduces pilot workload and enhances situational awareness.

From a regulatory standpoint, this architecture changes the emphasis of certification.

Fly-By-Wire As A Certification Discipline

Dassault's Digital Flight Control System (DFCS) reflects its established fly-by-wire philosophy exemplifies how aircraft functions have transitioned from mechanical linkage to algorithmic control. Pilot inputs are transmitted to flight control computers, which interpret commands and actuate control surfaces.

In such an environment, compliance is no longer demonstrated primarily through mechanical linkage integrity. Instead, certification authorities examine:

- Control law design and validation
- Redundancy architecture
- Failure-mode and degraded-mode behaviour
- Software assurance processes
- Traceability between requirements, code and test evidence

Fly-by-wire therefore becomes a systems safety case rather than a hardware narrative. The integrity of computing logic and its predictable behaviour across operating envelopes carries regulatory weight equal to that of structural design margins.

The Flight Deck As An Integrated Computing Platform

The NeXus / Primus Epic architecture incorporates advanced graphical flight planning, enhanced airport moving maps and runway overrun alerting functions, as described by Dassault and Honeywell.

These features depend on:

- Software processing performance
- Database integrity and update control
- Human-machine interface evaluation
- Alert prioritisation logic
- Configuration management discipline

Certification in this context extends beyond verifying equipment installation. It requires demonstrating that data inputs are accurate, that alerting behaviour is appropriate, and that updates to software or databases are controlled and assessed within a structured change-management framework.

Consequently, regulators now focus on the robustness of the engineering process: how requirements are captured, how traceability is maintained through design and verification, how regression testing is automated, and how configuration management controls change. This process-based certification acknowledges that software will evolve and that assurance must travel with every update without demanding complete re-certification of mature systems.

This is not experimental aviation. It is mainstream, high-end business aviation.

From "Born Digital" To Digitally Mature

Urban air mobility aircraft are frequently characterised as "software-first" because they integrate distributed propulsion, automation and digital control logic from inception.

The Falcon 10X shows that business aviation has already reached a comparable level of digital intensity. While its airframe and propulsion architecture are conventional, its control systems and cockpit environment reflect the same fundamental trends:

- Flight controls mediated by computing systems
- Integrated avionics rather than isolated subsystems
- Data-driven safety enhancements
- Automation dependent on rigorous software assurance

The certification question converges across sectors: can the applicant demonstrate that the integrated digital system is robust, traceable, reproducible and controlled?

The Falcon 10X offers a useful counterpoint to emerging air taxi narratives.
It shows clearly that:

- Software-intensive certification is not confined to special-class or experimental categories.
- Business aviation's flagship aircraft are deeply dependent on integrated computing.
- Fly-by-wire and digital flight decks require the same level of regulatory rigour as new-generation urban platforms.

In practical terms, the Falcon 10X confirms that aviation has entered a phase where airworthiness is as much about code integrity and systems integration as it is about structural strength and aerodynamic performance.

The Falcon 10X demonstrates that the future of aviation is software as much as structure. Its born-digital avionics and integrated systems highlight how airworthiness is becoming a disciplined synthesis of software assurance, systems engineering, and human-centred design. In this new paradigm, certification is not a one-time gate but a continuous partnership between regulators, manufacturers, and operators to ensure that digital innovations fly safely throughout their lifecycle.

As aircraft architectures grow smarter and more connected, the aviation industry's ability to certify software with the same rigour once reserved for physical hardware will define the next era of safe flight.

The industry discussion should therefore move beyond viewing "software-first" as a feature of future aircraft alone. In business aviation, it is already standard practice.

In short, flagship aircraft such as the Falcon 10X confirm that aviation has already entered an era where the integrity of code, data and integration logic carries the same regulatory weight as the integrity of metal and composite structures. That may be the most significant certification story of all.

PREDICTING THE DIGITAL FUTURE FOR COMMERCIAL AEROSPACE IN 2026

By Rob Mather VP Aerospace And Defence IFS

The commercial aerospace industry finds itself navigating two distinct transformations, says Rob Mather, VP of Aerospace & Defense, IFS.

On the ground, the priority is deep digital resilience: mitigating ransomware risks, easing supply chain bottlenecks with 3D printing, and augmenting a stretched workforce with Agentic AI. But look upwards, and there's a new era of physical expansion, where the rise of reusable launch vehicles is establishing a lucrative, unprecedented market for space MRO and logistics.

Prediction 1: The new cybersecurity imperative: Closing the vulnerable gaps in the tech stack

The entire commercial aviation network is critical. Its high-value infrastructure ensures the effective movement of people and goods around the world—think transportation of vaccines. The industry's vulnerability to cyberattacks and their ability to cause widespread disruption has been underscored by recent examples.

Here are the key developments to watch

Thales figures found a 600% increase in ransomware attacks in the aviation sector between 2024-2025. Just look to the ransomware attack in September 2025 that crippled check-in systems across multiple major European hubs such as Brussels, London, and Berlin!

At issue is the fact that aviation is still only digitally mature in part. The vulnerability lies in the "middle section"—where airline, aircraft, and ground systems have been partially modernized but are not fully up to date with modern cybersecurity practices.

Check out your software provider

In the year ahead, airlines and regulatory bodies, motivated by recent attacks and the essential role aviation plays in world affairs, and consequential potential targeting by state-sanctioned actors, will mandate a significant push for digital modernization across the entire industry. This will compel all major airlines and airports to implement up-to-date, modern cybersecurity practices for all operational systems, closing the "middle section" gap to counter potential threats.

Airline operators need seamless agility and resilience to stand any chance in the cybersecurity battle. Airlines and MROs must ensure their software provider constantly adopts a clear security posture, constantly addressing vulnerabilities with frequent updates using an evergreen approach, and ideally, designing out vulnerabilities from the beginning.

Prediction 2: Supply chain resilience: The rise of 3D printing & digital thread

Supply chain challenges for spare parts availability persist in commercial aviation, driving it back up to the top of the list of issues facing the aviation maintenance industry. Leading airlines and air operators to think outside the box and adopt innovative strategies to maintain operational readiness. One potential solution has been to use Parts Manufacturer Approval (PMA) parts, but some airlines face considerable hurdles here as lessors often refuse to allow OMA parts on their aircraft.

Even if used as a stopgap, airlines are forced to swap them out at time of lease return, meaning they are still subject to the main suppliers' limitations. However, other parts supply solutions are on the horizon.

At last, 3D printing goes mainstream

There are promising signs ahead of ongoing efforts by FAA and EASA regulators to clarify how 3D printed parts can be used in certain applications. Additive manufacturing, combined with the digital thread, could help solve supply chain bottlenecks by allowing parts to be produced quickly and in proximity to where

they are needed. In particular, this technology offers a solution for maintaining older aircraft more efficiently, as digital files for specific parts replace the need to store molds and retool assembly lines that may have been decommissioned years before.

Following a formal loosening of regulatory constraints, 3D-printed parts will become a mainstream, more accepted solution. The ability to rapidly produce both non-critical and older aircraft components will drastically streamline MRO processes and establish 3D printing as a driver of supply chain resilience in an industry that continues to feel the pain of supply chain issues.

We are already seeing this shift with certified 3D-printed engine components and heat exchangers that handle super-complex geometries not achievable through traditional manufacturing, such as those on the GE Catalyst turboprop engine and the 3-D printed air-to-air heat exchanger flying on the Cessna Denali.

Prediction 3: The Agentic era: Industrial AI provides a helping hand in the MRO hangar

It's abundantly clear that technician shortages will not be solved in the next 12 months. Despite technician certifications rising, The Pipeline Report from the U.S. Aviation Technician Education Council (ATEC) and Oliver Wyman shows increasing demand, and projected retirements are expected to leave commercial aviation with 10% fewer certified mechanics than needed in 2025.

So, the question becomes, how can we help the technicians we do have do more? One answer is to digitally augment the maintenance technicians to improve overall efficiency. This is where applications of Agentic AI are stepping up to the plate. One of the most impactful applications of this AI will be the creation of a "troubleshooting agent" to support maintenance technicians. This generative AI co-pilot will be able to navigate the extraordinary complexity of maintenance documentation, such as Airworthiness Directives (ADs) and Service Bulletins (SBs).

All hands on deck—including digital ones!

The ideal agent will be able help navigate complex reference documentation like AMMs, CMMs, troubleshooting manuals, or the IPC while pulling up pertinent SBs or ADs. The co-pilot could suggest it's a potential recurring fault and surface which repairs failed to work previously. Such a co-pilot could, in another scenario, suggest the likely candidates for troubleshooting tasks including historic success rates and time to execute. It could even request the required parts automatically, so they are there waiting.

In the year ahead, expect troubleshooting agents to move out of the pilot phase and into deployment within the maintenance operations of airlines and MROs. These agents will serve as a digital co-pilot that enhances the productivity of the existing, experienced workforce, while also helping close the knowledge gap for newer technicians.

Prediction 4: Beyond earth: The growth of the space aftermarket

Looking further skyward, an aftermarket opportunity is emerging that goes beyond Earth's stratosphere. The new aftermarket is being driven by a proliferation of satellites that have been deployed for communication, observation, and scientific purposes, combined with the rise of reusable vertical-landing rockets such as the SpaceX Falcon 9 and the newly developing Starship.

Commercial space tourism is now adding a third catalyst, with reusable spaceflight vehicles that must be maintained to rigorous safety and compliance standards between flights. Together, these shifts are creating an entirely new MRO market for launch platforms themselves, which now require a formal sustainment process rather than simple disposal after a single use. MRO in space!

For the most part, orbital vehicles have been treated as disposable assets with a finite operational life. Bringing spacecraft back down to Earth has not been feasible, and sending repair systems up has been equally impractical. The advent of self-healing materials is beginning to shift this paradigm by enabling spacecraft to autonomously repair micro-cracks and structural degradation in orbit, as demonstrated in recent aerospace research on self-healing composites. At the same time, dramatically lower launch costs mean that in-orbit servicing and repair are becoming feasible for the first time.

Launch and space-platform MRO is rapidly emerging as the next frontier. Blue Origin's multi-use Blue Ring platform illustrates how reusable vehicles will create entirely new sustainment markets. In parallel, NASA's On-Orbit Servicing, Assembly and Manufacturing (ISAM) framework highlights how satellites and launch systems will require formal sustainment infrastructures rather than being treated as disposable.

Research shows the Space Logistics Market Size will grow to $19.8 billion by 2040, with large growth driven by on-orbit servicing, assembly and manufacturing, as well as last-mile logistics. The ripple effect over the coming years is that these once disposable space assets will require sustainment and support strategies to maximize availability, efficiency, and further reduce the costs of space operations. This means maintenance needs to be built into the asset management lifecycle. Manufacturers must make sure vehicles are ready not just for use, but for re-use and critically, are 100% operational when they are required.

The digital imperative

Establishing a strong digital foothold now can not only allow commercial aerospace organizations to leverage currently available tools for 3D printing and AI-enabled MRO, but they can also enter a new stratosphere as space becomes the next frontier for aftermarket opportunity.

Long Range VT35. Image Courtesy of: eHANG

AUTONOMY FIRST: WHY UNCREWED AVIATION BECAME THE TEST BED FOR SOFTWARE FLIGHT

Uncrewed aviation did not begin as a philosophical shift in flight control. It began as a practical one. Remove the onboard pilot and the safety buffer changes. Decision-making authority moves from cockpit instinct to software logic, command links and predefined operating envelopes.
In doing so, uncrewed aircraft systems (UAS) became aviation's first large-scale experiment in software-defined flight.

Collision Exposure: When Separation Becomes A System Problem

International incident reporting demonstrates that uncrewed aircraft are no longer operating at the margins of aviation risk.

In the United States, the National Transportation Safety Board has investigated collisions between small unmanned aircraft and helicopters operating at low altitude. In one case, a helicopter conducting operations at an off-airport landing zone sustained substantial rotor blade damage following impact with a UAS. In another investigation, probable cause was attributed to the remote pilot's failure to give way to the helicopter.

Such events underline a structural reality: low-level airspace is shared by helicopters, emergency services, law enforcement and inspection aircraft. The risk is not theoretical. It is operational.

For uncrewed systems, separation cannot rely on see-and-avoid. It must be engineered through geofencing, detect-and-avoid logic, procedural containment and airspace coordination.

Autonomy therefore becomes not a performance feature, but a safety mechanism.

Regulatory Stress Points: Formalising Software Authority

As UAS operations expand, regulators are being compelled to define governance structures for autonomy at scale.

In the United States, the Federal Aviation Administration has proposed rulemaking intended to normalise beyond visual line of sight (BVLOS) operations. The issue is not simply range extension. It is accountability: who is responsible for separation, what technical performance is required, and how systemic risk is managed.

In Europe, the European Union Aviation Safety Agency applies the Specific Operations Risk Assessment (SORA) methodology for higher-risk operations. This approach shifts approval from aircraft-centric certification toward structured risk classification and mitigation design.

Remote identification requirements add another layer, linking traceability and enforcement to operational legitimacy.

These frameworks represent stress points because they formalise what was once informal: the transfer of behavioural authority from pilot judgement to system design.

Human Factor Shift: Operator To Supervisor

Uncrewed aviation alters not only aircraft design but human roles.

The remote pilot increasingly functions as a system supervisor rather than a direct controller. Safety performance is defined before flight through:

- Operational design domain limitations
- Geographical constraints
- Contingency logic
- Command-link redundancy
- Pre-flight risk assessment

Competence is measured less by control dexterity and more by risk modelling, procedural compliance and exception management.

In effect, the human becomes part of the safety architecture rather than the primary safety buffer.

Public Trust And Societal Acceptance

Autonomy does not exist in technical isolation. Its sustainability depends on public trust. Research across Europe and the United Kingdom indicates that public support for drones is strongly linked to mission type. Emergency response, search and rescue and infrastructure inspection attract higher acceptance.

Routine delivery or persistent surveillance generates more conditional support, often tied to concerns around safety, noise and privacy.

Acceptance therefore follows perceived public benefit and confidence in governance.

Incidents — particularly collisions or airspace infringements — resonate beyond technical consequence. They shape societal tolerance.

Uncrewed aviation is thus not only a regulatory test bed. It is a social one.

Why Uncrewed Aviation Leads The Software Transition

The reason UAS became the proving ground for software flight is structural.

In a conventional aircraft, a pilot can compensate for unexpected behaviour. In an uncrewed aircraft, behaviour must already be defined, bounded and recoverable without physical intervention. This necessity has accelerated:

- Detect-and-avoid development
- Command-link resilience
- Operational containment strategies
- Performance-based regulatory frameworks
- Digital identity and traceability mechanisms

These disciplines are now influencing broader aviation governance, including emerging autonomy integration in larger aircraft categories. Uncrewed systems moved first not because they were simpler, but because they could not rely on onboard human redundancy.

Autonomy in aviation did not begin with ambition. It began with absence — the absence of a pilot in the cockpit.

That absence forced regulators, engineers and operators to formalise software authority, define performance thresholds and construct structured safety cases for behaviour under uncertainty.

Uncrewed aviation therefore stands as the primary laboratory for software-defined flight.

The lessons emerging from collision exposure, regulatory stress points, human role transformation and societal acceptance are not confined to drones.

They represent an early chapter in aviation's broader transition toward software-governed safety architecture.

AVIATION CLOUD MARKET

By Niopal Ojha. Assistant manager Aerospace and Defence Research.

Cloud computing is often discussed in commercial terms — scalability, cost efficiency and digital transformation. Yet within aviation, the shift to cloud-based infrastructure carries deeper operational implications.

As aircraft systems become increasingly software-dependent and data-driven, the underlying computing environment supporting those systems moves further from traditional, physically controlled infrastructure.

Flight operations, maintenance planning, passenger systems and manufacturing analytics are now routinely processed through distributed cloud environments.

This structural shift raises important questions for regulators, operators and system designers alike. When operational logic resides beyond the perimeter of airline-owned servers, resilience, redundancy and cybersecurity become matters of operational assurance — not merely IT strategy.

In an era where code integrity, data governance and system validation are assuming equal weight to mechanical certification, cloud infrastructure forms a critical, if largely invisible, layer within the aviation ecosystem.

The following contribution examines the growth and drivers of the aviation cloud market. Read within the broader context of this edition's focus on digital oversight and system integrity, it highlights how foundational infrastructure is quietly reshaping the way aviation operates.

According to MarketsandMarkets, the aviation cloud market is experiencing sustained growth, driven by increasing adoption of cloud-based solutions across airlines, airports and aerospace manufacturers.

Cloud computing offers operational scalability, cost efficiency, flexibility and enhanced collaboration. As digital transformation deepens across aviation, cloud infrastructure is becoming integral to operational management, data processing and service delivery.

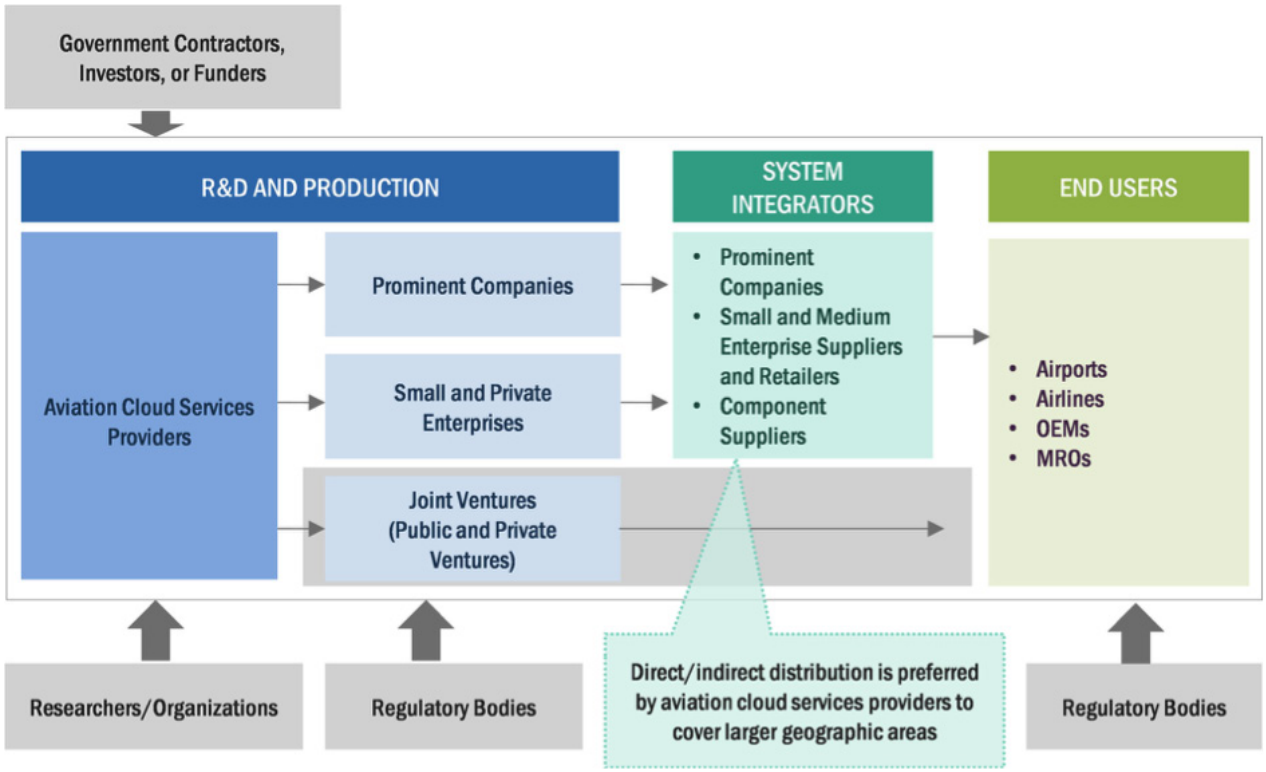
Key market participants are incorporating artificial intelligence (AI), machine learning (ML) and advanced analytics into cloud platforms to support flight operations, maintenance planning and passenger services. As aviation becomes progressively data-intensive, cloud technologies are positioned as foundational infrastructure rather than optional enhancements.

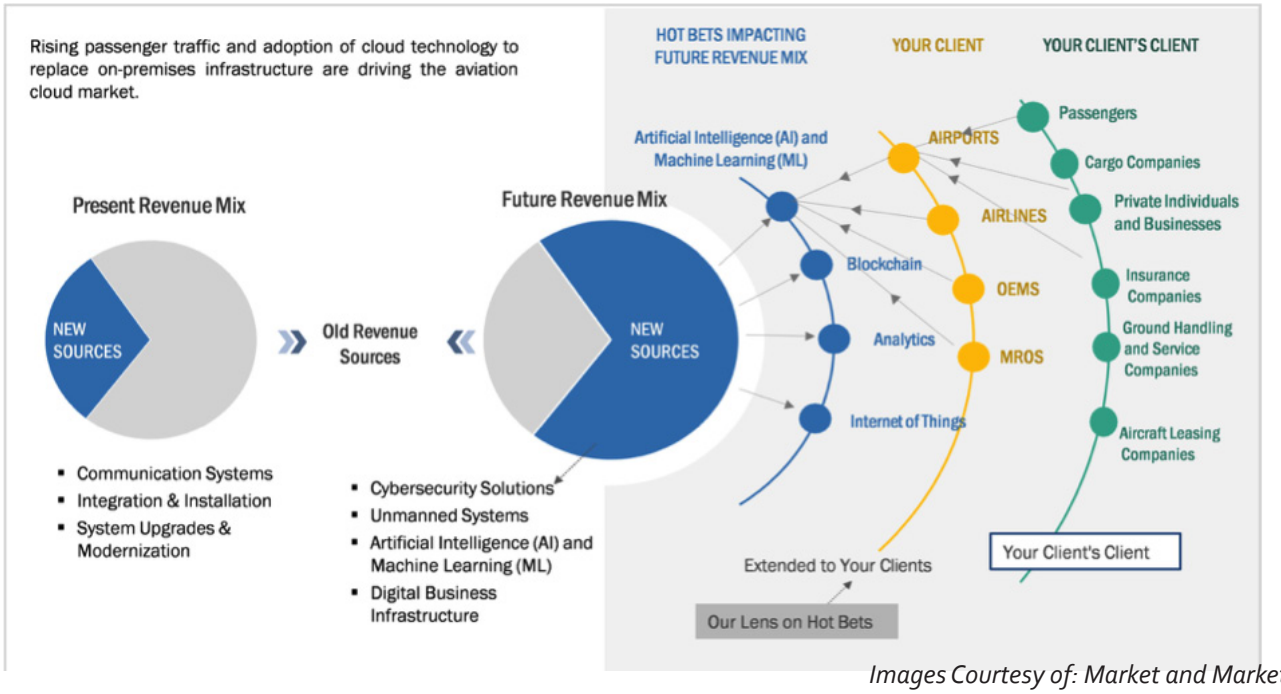
Aviation Cloud Market Ecosystem

Growth in global passenger traffic continues to increase the complexity of aviation operations. Airlines generate extensive datasets across scheduling, bookings, crew management, maintenance tracking and regulatory compliance. Managing this data efficiently requires scalable computing environments capable of processing large volumes in real time.

Cloud platforms provide the elasticity necessary to store, process and analyse operational data without requiring extensive physical infrastructure. This enables improved decision-making, predictive analytics and operational optimisation.

Passenger expectations have also evolved.





Images Courtesy of: Market and Markets

Cloud-based customer relationship management (CRM) systems support personalised services, loyalty programme management and multi-channel communication. While these systems enhance engagement and revenue opportunities, they also demand secure, resilient and high-availability infrastructure.

The increasing reliance on cloud computing reflects the sector's need to manage operational complexity while maintaining efficiency and regulatory compliance.

Revenue Shift In Aviation Cloud Market

Migration from legacy on-premises infrastructure to cloud services

The aviation industry is progressively migrating from legacy on-premises systems to cloud-based environments. This shift is largely driven by scalability requirements, cost considerations and the need for operational agility.

Traditional IT infrastructure involves substantial capital expenditure on hardware procurement, system maintenance and upgrade cycles. Cloud models, by contrast, operate on a usage-based structure, allowing aviation stakeholders to align expenditure with demand.

This flexibility is particularly relevant in a sector subject to seasonal variability and external disruptions.

Scalability is a further consideration. Airlines and airports must accommodate fluctuating passenger volumes, operational peaks and increasing data generation. Cloud platforms allow resources to expand or contract dynamically, supporting continuity during peak demand while avoiding unnecessary infrastructure costs during quieter periods.

Aircraft manufacturers are also adopting cloud technologies to support design, engineering, supply chain coordination and production management.

Aircraft development involves large-scale simulations, collaborative engineering and global supplier integration. Cloud-based computing environments enable distributed teams to collaborate in real time, manage version control and accelerate decision-making processes.

In April 2022, Boeing announced technology agreements with Google Cloud, Microsoft and Amazon Web Services (AWS). The company selected Google Cloud to migrate multiple applications across business units, utilising automation, data analytics and AI/ML capabilities to improve manufacturing and operational efficiency. Boeing also adopted Microsoft Cloud for infrastructure modernisation and mission-critical systems, while extending existing operations with AWS.

These partnerships illustrate how cloud providers are becoming embedded within aerospace production ecosystems.

Service Unavailability Risks

Despite operational advantages, cloud service dependency introduces systemic risk. Service unavailability can occur due to technical failures, network disruptions, cyber incidents or natural events.

When outages affect aviation systems, operational consequences may be immediate.

Airlines rely on cloud-based platforms for scheduling, booking, dispatch coordination and maintenance tracking. Downtime can result in flight delays, cancellations and increased operational cost. Airports and air navigation service providers similarly depend on cloud-hosted analytics and operational planning systems.

In June 2023, AWS experienced a multi-hour outage affecting numerous users globally. According to outage monitoring service Down Detector, approximately 11,500 reports were logged at the peak of disruption.

Such incidents highlight operational exposure when critical services depend on third-party cloud infrastructure.

Repeated service interruptions may undermine stakeholder confidence and expose providers to reputational and commercial risk. As reliance increases, resilience, redundancy and disaster recovery planning become essential components of aviation cloud strategies.

Data Security And Privacy Concerns

Data protection remains one of the most significant constraints on aviation cloud adoption. The sector operates under stringent regulatory frameworks, including International Civil Aviation Organization (ICAO) standards, Federal Aviation Administration (FAA) requirements and data protection regulations such as GDPR.

Aviation systems are highly interconnected. Vulnerabilities in one system can potentially affect broader operational networks. Cyber threats targeting reservation systems, operational control platforms or air traffic services could disrupt flights and compromise sensitive information.

Cloud environments must therefore implement robust cybersecurity architectures. These include encryption protocols, identity and access management (IAM), network segmentation, intrusion detection systems and continuous vulnerability assessment.

The increasing integration of Information and Communication Technology (ICT) into aviation systems has expanded the threat surface. Research published by MDPI in March 2022 highlighted growing vulnerabilities as aviation systems become more interconnected. Advanced Persistent Threat (APT) groups, in particular, target intellectual property and critical infrastructure through sustained cyber campaigns.

The proliferation of connected devices; including aircraft sensors, ground systems and passenger technologies, further complicates cybersecurity management. Securing these endpoints within cloud ecosystems requires comprehensive monitoring and layered defensive measures.

While cloud providers invest heavily in security infrastructure, aviation stakeholders must ensure regulatory compliance and maintain governance oversight when migrating sensitive operations to external environments.

Ai-Enabled Cloud Analytics

The incorporation of AI-based analytics within cloud platforms represents a significant development in aviation operations.

Predictive maintenance is one prominent application. By analysing historical maintenance records alongside real-time aircraft sensor data, algorithms can identify patterns indicative of component degradation. Early detection supports proactive maintenance scheduling, reducing unplanned downtime and enhancing reliability.

Cloud-based AI systems are also being applied to flight operations optimisation. By integrating weather data, airspace conditions, congestion patterns and fuel performance metrics, route planning can be adjusted in real time. The objective is to improve efficiency, reduce fuel burn and enhance schedule adherence.

In May 2023, Qatar Airways and Google Cloud announced a collaboration to leverage data analytics and AI tools, including BigQuery and Vertex AI. The initiative aims to enhance passenger experience, streamline operations and support sustainability objectives through digital optimisation. Such partnerships demonstrate how AI-enabled cloud platforms are being integrated into airline transformation strategies.

These developments reflect a broader shift toward data-driven operational models, where cloud infrastructure supports continuous performance refinement.

Cloud adoption is particularly evident within maintenance, repair and overhaul (MRO) operations. Cloud-based MRO IT platforms provide real-time data access, integrated maintenance tracking and enterprise-wide coordination.

One reported advantage is the elimination of dedicated physical server infrastructure, reducing capital expenditure and IT maintenance overhead. For airline operators, Continuous Airworthiness Management Organisations (CAMOs) and independent MRO providers, this shift can simplify system administration and improve scalability.

Cloud-based maintenance platforms support integrated airworthiness management, parts tracking and regulatory compliance documentation. Enhanced analytics capabilities assist with predictive maintenance planning and risk identification, contributing to operational reliability.

By centralising data within accessible environments, cloud-based MRO systems enable faster decision-making and reduced aircraft downtime. The result is improved operational efficiency and strengthened safety oversight.

As reliance on digital maintenance platforms increases, integration standards, data governance and regulatory compliance remain critical considerations.

Market Outlook

The aviation cloud market is projected to grow at a compound annual growth rate (CAGR) of 16.1% over the forecast period. Growth drivers include AI, machine learning, analytics, blockchain applications and Internet of Things (IoT) integration. However, expansion is balanced by structural risks, including service reliability, cybersecurity exposure and regulatory oversight requirements.

Cloud computing is no longer peripheral to aviation operations. It is becoming embedded within flight operations, manufacturing, maintenance and passenger services. The market's trajectory will depend not only on technological innovation, but also on the sector's ability to maintain resilience, data integrity and regulatory compliance within increasingly complex digital ecosystems. *INFO: https://www.marketsandmarkets.com*

AERO
SOUTH AFRICA

10-12 JUNE 2026

Lanseria International Airport,
Johannesburg, South Africa

YOUR AVIATION COMMUNITY TRADE SHOW

EXHIBIT WITH US

www.aerosouthafrica.com

@aero_south_africa
@AERO Expo South Africa
@AEROSouthAfrica1
@AEROExpoSA

In co-operation with
fairnamic

Partner
ASP
ADRENALINE SHOW PRODUCTIONS

Venue Partner
LANSERIA
INTERNATIONAL AIRPORT

Media Partner
AIRNEWS

Organised by
messe frankfurt

ETION CREATE SHOWCASED MISSION ARCHITECTURE IN RIYADH

Image Courtesy of: ETION create

At the recently concluded World Defense Show 2026 in Riyadh, South Africa's Etion Create presented a suite of tactical navigation and cybersecurity systems highlighting the increasing role of software-defined architecture in operational aerospace and defence environments.

Pretoria-based electronics company Etion Create exhibited at the third edition of the World Defense Show (WDS2026), held in Riyadh from 8 to 12 February.
The company presented a range of cybersecurity and tactical navigation solutions, including the debut of its Cheetah tactical router.

Built on the VNX+ platform, the router is ITAR-free and compliant with NATO Generic Vehicle Architecture (NGVA) standards, positioning it for tactical vehicle applications.

Importantly, the system has a defined upgrade path into mission computer applications. According to Tobie van Loggerenberg, Executive: Business Development Manager, the platform can be upgraded using either a CM120 Intel Atom module or an NVIDIA Jetson Nano VNX+ processing module.

The router provides centralised encrypted connectivity supporting situational awareness, sensor and effector interfacing, internal and external vehicle communications, and tactical datalink functions.

The approach reflects a broader industry shift towards scalable processing platforms, where operational capability evolves through software-enabled modules rather than fixed-function hardware replacement.

Navigation Resilience In Gnss-Denied Environments

Also displayed was the CheetahNAV Compact, a more cost-effective and space-efficient version of the established CheetahNAV tactical vehicle navigation system.

Designed for integration into compact vehicle platforms, the system incorporates real-time moving map technology to provide continuous situational awareness to operators.

In GNSS-denied conditions, the navigation solution delivers dead-reckoning horizontal accuracy of 0.2% of distance travelled — approximately 200 metres over 100 kilometres.
An integrated inertial measurement unit (IMU) enables continued operation during jamming or emergency scenarios where normal communications networks are compromised.
CheetahNAV systems are now being built in Saudi Arabia and are in service within the Kingdom and with regional customers, reflecting the Middle East as a strategic focus area for the company.

Encryption as a system layer

On the cybersecurity front, Etion Create presented the RQ11 system, designed to apply a blanket layer of encryption over existing radio networks.

Intended for command centres, base or shore stations and naval vessels, the RQ11 enables secure and interoperable voice and data services across radios from diverse manufacturers.

All over-the-air communications are encrypted, with access controlled via an access code. A dedicated Crypto/Plain switch and indicator lights provide operational clarity, while a Zeroize function allows complete erasure of data and keys from the front panel.

The system is based on Etion Create's TQ5 secure modem module and the Nanoteq QCM-R radio cryptographic module, providing auditability within the secure cryptographic architecture.

Rather than replacing existing hardware networks, the RQ11 operates as an encryption overlay, reinforcing a systems model in which resilience and interoperability are governed through integrated processing and cryptographic control.

Positioning Within A Broader Technology Ecosystem

Etion Create has incorporated Nanoteq Products and Engineers and operates within the South African Reunert Group's Reutech Applied Electronics division.

As an original design manufacturer with international reach, the company serves defence and aerospace, information security, mining, rail and industrial sectors.

Its participation at WDS2026 highlighted a consistent architectural theme: navigation, communications and mission control are increasingly structured around integrated processing platforms and encrypted connectivity frameworks.

In this environment, hardware remains visible — but operational authority and resilience are increasingly defined by software-driven systems architecture.

Garmin GHA15. Image Courtesy of: Garmin

WHEN HEIGHT BECOMES DATA

Garmin's GHA 15 shows how even fundamental flight parameters are becoming software-defined

A Practical System With Broader Implications

Garmin has introduced the GHA 15 height advisor, a radar-based system designed to provide above-ground-level (AGL) altitude reference for general aviation, experimental and light sport aircraft.

The unit delivers digital AGL advisory readings from 500 feet to touchdown on compatible displays. Audio callouts provide landing cues at selected intervals from 300 feet down to 1 foot AGL when connected through supported systems.

On the surface, it is a practical enhancement to landing awareness. Structurally, it reflects a broader shift in avionics: altitude is increasingly defined by processed sensor input rather than pressure-derived estimation alone.

From Signal To Continuous Data Stream

The GHA 15 operates by transmitting radio waves downward from the aircraft. When the signal reflects from the surface below, the system determines precise height using the time delay of the returned signal. Unlike traditional barometric instruments, which depend on atmospheric pressure settings, the radar-based system provides direct measurement relative to terrain or water.

The system processes hundreds of altitude measurements per second and applies advanced digital filtering to maintain a smooth and continuous AGL reading. Height awareness therefore becomes a continuously processed data stream — stabilised and interpreted before it reaches the pilot.

Integrated Into The Avionics Ecosystem

The compact module, slightly larger than a deck of cards and weighing less than 0.45 kg, integrates the antenna and radar transceiver into a single self-contained unit for installation on the underside of the aircraft.
In experimental and light sport aircraft, the GHA 15 is compatible with Garmin's G3X Touch flight displays. It is also approved to interface with the GI 275 flight instrument in select Class I and II certified aircraft, subject to required equipment configurations.

Digital readouts display on supported G3X Touch primary flight displays and GI 275 ADI, HSI, MFD and standby ADI variants. Audio outputs integrate with compatible audio panels, intercoms or headsets.

Rather than functioning as an isolated instrument, the system operates within an integrated display environment where sensor input, processing logic and cockpit presentation are aligned.

Small System, Structural Shift

For pilots, the practical benefit is enhanced situational awareness during approach and landing, particularly in areas where current barometric altimeter settings may not be readily available.
For the industry more broadly, the significance lies in the architecture.

Even fundamental flight parameters such as height above terrain are increasingly derived from sensor fusion and digital filtering rather than a single instrument source. The GHA 15 is not an OEM-scale platform or complex automation suite. It is a compact general aviation device. Yet it illustrates the same transition visible across modern flight decks: aviation systems are steadily moving from hardware-led instruments to software-defined information environments.

Not every structural shift arrives in the form of a new airframe. Sometimes it appears in a module the size of a deck of cards.

For more information visit: https://www.garmin.com

Image Courtesy of: ARCHDaily

FROM AIRFIELDS TO AEROTROPOLISES

How the humble airstrip transformed into the mega-airport.

By Alexey Rodokanakis

Airports have become almost unrecognisable from their humble aerodrome beginnings in the early 20th century, when they were often little more than a strip of turf and a rudimentary windsock. The first recorded use of the word "airport," though somewhat contested, appeared in the Brooklyn Daily Eagle in 1902, soon after aviation pioneer Alberto Santos Dumont (heir to a Brazilian coffee dynasty and designer of some of the first long-distance dirigibles) coined the term as describing a port for airships. The term only gained its more modern connotations in 1919 when journalist Robert Woodhouse used it to describe Bader Field in Atlantic City, a location accommodating both land-based aircraft and seaplanes travelling to New York.

Irrespective of its exact etymology, there is little doubt that denizens of the first quarter of the 20th century would scarcely recognise the airports of today. These are now massive edifices of intercontinental trade and travel — more like highly secure, cavernous shopping malls than the dusty and remote patches of earth of yesteryear.

There is some debate about when this transition from simple airstrip to lifestyle complex truly occurred, though general consensus places it squarely in the heady boom years of the post-war period, the 1950s to be precise. After the first wave of gourmet dining


Image Courtesy of: WSJ

Image Courtesy of: DOMUS

establishments — fittingly introduced in an age when air travel was an exclusive and luxurious endeavour — had ensconced themselves within every respectable airport, the introduction of duty-free shopping marked the next major addition. This forever transformed the airport from a mere entry and exit point into a place where new offerings encouraged travellers to linger for more than the brief moment required to catch their flight.

The massive increase in air travel brought about by higher-capacity passenger aircraft and jet turbine engines in the mid-20th century meant that airports needed to become far more strategically designed. They now had to channel travellers effectively from landside to airside while ensuring that checking in luggage, moving through passport control, and browsing the growing array of shops could occur as seamlessly as possible. This necessity led to the next major innovation in airport design: "Stage Development."

The TWA Flight Center at JFK Airport, designed in 1962 by Eero Saarinen, not only shifted airport architecture away from a collection of grey utilitarian boxes but laid the foundations for a revolution in the functioning of interior airport spaces. The building itself, with its four interlinked concrete vaults, resembles a giant abstract bird poised to take flight, serving as a symbolic monument to aviation. Its thin-shell concrete construction allowed for an interior space almost entirely uninterrupted by walls and columns. This was the first true instance of the airport hall, the grand, hall-like space that has become ubiquitous in modern airports.

What began as an architectural evolution in form and passenger experience would, over time, become something more consequential. As airports grew in scale and complexity, spatial design was no longer merely aesthetic or symbolic; it became operational logic. Saarinen carefully segmented the passenger journey: from the public, landside arrival zone with its access roads and parking, through a "hinging" area where passengers undergo a change in legal status by checking in and passing through security, and finally into the secure airside. Here travellers could make free use of duty-free retail hubs, bars, restaurants, and lounges while awaiting departure. Saarinen is also responsible for integrating innovations such as jet bridges, baggage carousels, and the now-phased-out split-flap display boards — the kind that flip over like old calendar clocks, a true aesthetic loss.

Today, airports function not only as ports of entry for their respective countries but as symbols of those countries themselves. Many governments and city administrations now spend hundreds of millions, if not billions, to outdo one another in airport design and scale.

If they succeed (and pair their efforts with a well-run national carrier) they can secure their airports' positions as international hubs not only for connecting flights but as symbolically desirable destinations in their own right.

Following the rapid growth of Emirates Airline in the early 2000s, a decision was made to massively modify and enlarge Dubai International Airport (DXB) to 2.12

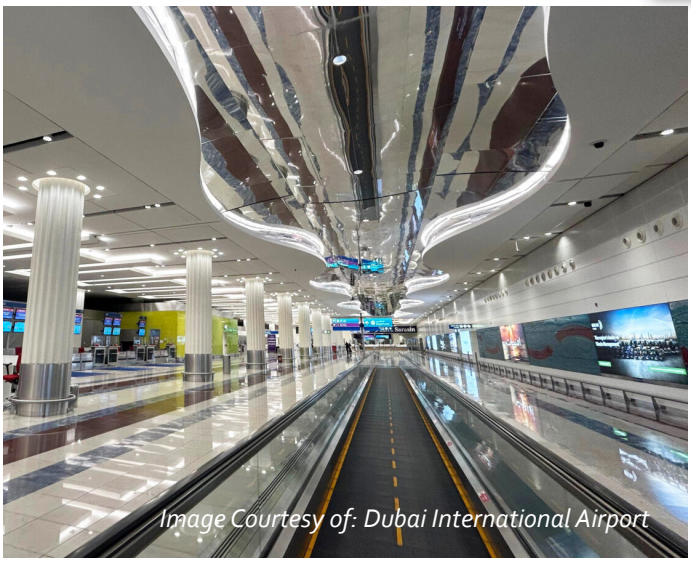


Image Courtesy of: Dubai International Airport

million square metres of built-up area. It was a risky decision, but one that paid off spectacularly when, in 2014, DXB surpassed London's Heathrow to become the busiest airport for international passengers, handling over 70.4 million travellers that year and 95.2 million last year. Authorities now plan to move operations to the new and much larger Al Maktoum International Airport (DWC) by the 2030s to further increase capacity. This mega-airport will have a total built area five times that of DXB, span 140 square kilometres, and handle up to 260 million passengers annually, undoubtedly becoming the world's largest airport.

In an age of ever-evolving technology, advanced air-management systems, and design approaches driven by building-integrated modelling and artificial intelligence, competition now lies not just in scale and capacity but in efficiency. Airports of modern proportions pose extreme logistical challenges that must be carefully managed to keep the wheels turning. A leading example of this is Singapore Changi Airport, which has woven advanced technology into virtually every layer of its operations.

From automated early-bag-drop systems and AI-assisted crowd-flow modelling to biometric immigration clearance and predictive maintenance for everything from baggage systems to air-conditioning loads, Changi demonstrates how intelligent design and real-time data can enhance passenger flow, reduce bottlenecks, and sustain efficiency even as traveller numbers continue to climb.

As airports continue to evolve, their function as gateways is increasingly augmented by their role as microcosms of modern society — places where technology, culture, and commerce converge in ever more sophisticated ways. The relentless march toward greater connectivity and efficiency has transformed these once humble airfields into global hubs, shaping both the journeys and the experiences of millions. In essence, our airports have become reflections of our ambitions: ever reaching, ever adapting, and always striving to be more than mere points of transit. Whether viewed from the air or approached from the ground, they remain enduring symbols of human ingenuity and the unceasing desire to travel further and dream bigger.

SYSTEMS MANAGER OR PILOT?

When software becomes the pilot.

By Rob Garbett

I have drawn on insights from friends and technical experts in addressing this complex subject, which lies beyond my direct operational experience.

A colleague trained in 1962, later a Captain on the Boeing 747-400 and still active in private flying, reflected:

"I was required to acquire an intense knowledge of software-dependent automation. The transition was difficult. However reliable the instrumentation, manual flying skills must be maintained and audited."

The early Airbus A320 accident at Mulhouse in 1988 demonstrated how misunderstanding automated flight modes can have fatal consequences. During a low-level flypast, misinterpretation of flight control modes and aircraft energy state resulted in controlled flight into terrain. Sophisticated protection systems did not compensate for incomplete system awareness.

Air France Flight 447, an Airbus A330 operating from Rio de Janeiro to Paris in 2009, reinforced that lesson. Pitot tube icing led to unreliable airspeed indications and autopilot disengagement. The aircraft subsequently entered a high-altitude stall. The crew did not recognise the condition in time to recover.

The accident highlighted the continued importance of manual flying competence and a clear understanding of flight envelope protections.

The Boeing 737 MAX accidents further illustrated how flight control software, when triggered by erroneous sensor data, can generate aircraft responses crews may not immediately anticipate. Subsequent investigations examined not only system design, but also training assumptions and certification oversight.

Glass cockpit technology represents a significant advance over analogue instrumentation. Modern Flight Management Systems reduce workload, optimise performance and enhance precision. Aircraft such as the Airbus A350 and Boeing 787 are capable of highly automated operations under appropriate conditions.

Yet multiple failures remain possible. In such circumstances, the pilot must understand system architecture and retain the ability to fly manually.

Training therefore becomes central. Pilots must not simply follow screen indications without deeper comprehension. Commercial pressures are real — classroom time does not generate revenue — but cost control must not erode competence.

Manufacturers face similar tensions. Increased automation improves efficiency and reduces workload, and fleet commonality lowers costs. However, subtle differences between aircraft variants can create cognitive overload if not fully understood.

Earlier generations of technical training demanded detailed systems knowledge — the "nuts and bolts" approach. Today, there can be an assumption that automation will manage complexity if properly engaged.

The late General Des Barker frequently cautioned against "automation fixation". Even in general aviation, advanced autopilots and safety systems are increasingly available. These are valuable innovations, but without skill and judgement they may not provide the safety margins assumed.

As he observed:

"Pilots of the automation generation — the 'pilots of the magenta line' — will need technical knowledge approaching that of an engineer. Without full understanding of integrated systems, pilots risk being at the mercy of automation following failures."

Captain Chesley "Sully" Sullenberger has similarly noted:

"If we only look at the pilots — the human factor — then we are ignoring other important factors; we have to look at how they work together."

Automation has unquestionably enhanced safety, efficiency and precision. It is not the adversary.

But when manual flying skills diminish, automation can become a vulnerability rather than a safeguard.

There is a familiar quip: why two pilots? One to monitor the autopilot, and one to ensure the first does not touch anything.

Behind the humour lies a serious question.

As aircraft become increasingly software-defined, are we training systems managers — or pilots?

The Commercial Aviation Association of Southern Africa

CAASA is a non-profit organisation formed in 1944 to promote and protect the commercial interests of the general aviation industry in South Africa

Melissa Sewgolam

Mobile: +27 (0) 82 847 3403

Email: mellisa@caasa.co.za

Gate 9, Lanseria International Airport

www.caasa.co.za

Looking to showcase your brand to a highly engaged audience of aviation professionals, enthusiasts, and industry leaders? World Airnews offers premium advertising opportunities across our print and digital platforms—ensuring your message reaches the right people, at the right time.

Don't miss your chance to be featured in our next edition.

Contact us today to explore advertising options:
Email: advertising@worldairnews.co.za
Web: https://worldairnews.co.za/advertise/
Call: 011 465 7706

World Airnews – Connecting Skies • Bridging continents