Aviation voice networks span multiple organisations, technologies, and environments
Frequentis

Safety first

In an increasingly interconnected ATM landscape, the shift from isolated analogue frequencies to IP-based networks has rewritten the risk profile of mission-critical communications, explains Frequentis' Bernd Bösendorfer-Baldun

Voice security in aviation is fundamentally different from traditional IT security because the data involved is not simply information, but a real-time operational conversation that directly affects safety. Crucially, aviation voice networks span multiple organisations, technologies, and environments, from cockpit radios and satellite links to ground communication systems and air traffic control centres. Securing that chain requires more than traditional IT protections. It calls for operational understanding of how communication flows in safety-critical environments.

Risk mitigation

Stolen voice or configuration data could potentially provide attackers with the critical operational intelligence needed to analyse air traffic patterns, identify emergency protocols, or prepare for 'spoofing' attacks. Preventing these vulnerabilities is the primary driver behind our 'Trusted-Zone Security' architecture. At Frequentis, we recognise that modern VoIP-based ATM operates within a complex IT landscape that demands a holistic approach to network integrity. A key driver of this collaborative shift is the EUROCONTROL VoIP Security Baseline (2020), which defines the framework for network segmentation and access control, ensuring that critical voice paths remain strictly isolated from administrative traffic.

The baseline provides the industry with an essential framework for outlining risks, evaluating their impact, and defining further actions. This includes addressing threats such as active manipulation tactics (eg SIP spoofing or registration hijacking), operational failure due to cyberattacks (such as targeted DoS designed to overwhelm gateways), and unauthorised changes to network architecture or access control lists.

In an interconnected landscape, the focus of security has shifted towards ensuring the absolute authenticity of communication. Certificate-based identity verification is essential to ensure that instructions remain untampered and that no unauthorised actor can digitally 'imitate' a controller or pilot. This is why our 'Trusted-Zone Security' architecture builds these protections directly into the system's logic.

Our X10 voice communication system and the MosaiX platform were engineered with native, deep-integrated

Bernd Bösendorfer-Baldun is director of the Market Unit Voice Solutions at Frequentis

resilience. Security is not an additional layer. It is the foundation upon which the entire system architecture is built. This ensures that critical security mechanisms – such as certificate-based authentication and controlled access to interfaces – are built directly into the system's logic rather than added later.

A change in mindset

Historically, air traffic control communications relied heavily on physical and network isolation, but modern ATM is increasingly digital and interconnected. Remote towers, digital data sharing, integrated ATM systems, and IP-based communications all require systems to interact across networks that were previously separate.

The biggest shift in mindset is therefore from security through isolation to security, through resilience and controlled connectivity.

This means adopting layered security architectures where authentication, encryption, network segmentation and monitoring work together to protect communications while still allowing the necessary operational data flows. At the same time, systems must be designed to continue operating safely even if parts of the network are disrupted or under attack.

For mission-critical communications providers like Frequentis, this transition has required a shift from purely telecoms-style system engineering towards cyber-resilient operational platforms. Security must be integrated into the system architecture from the outset, ensuring that controllers and pilots can continue communicating seamlessly as the surrounding infrastructure becomes more connected.

How can we layer on high-level security without introducing the kind of latency that could interfere with pilot-controller safety? From a technical perspective, voice transmitted over IP networks may appear similar to any other packet of data. In operational aviation environments, however, voice communication carries unique performance requirements.

Pilot-controller exchanges depend on immediacy and clarity. Even small delays can disrupt the communication flow or increase cognitive workload for controllers managing busy airspace.

For that reason, the security mechanisms used in voice communication systems must be specifically engineered for real-time environments. Standard enterprise security (like some VPNs) adds heavy headers to every packet. For aviation, we adhere to internationally mandated standards like ED-137 (the global standard for VoIP in ATM). Frequentis systems use strict QoS [Quality of Service] tagging to ensure voice packets "jump the queue" ahead of less critical data.

Rules and regulations

The shift from legacy analogue systems to Voice over IP (VoIP) is the most significant technical change in the history of ATM. While this transition allows better flexibility and integration across borders, it fundamentally changes the security profile of the sky. As Frequentis ensures the safety of 95% of the world's passengers and aircraft, our experience reflects how these regulations translate across different borders.

For the global market, the primary challenge is ensuring that as voice becomes 'data', it remains shielded from the delays and cyber risks inherent in digital networks. To address this, the industry is increasingly moving towards the ISO/IEC 27001 framework for organisational security, while simultaneously adopting ATM-specific technical standards such as EUROCAE ✈

Voice data must be safeguarded so that attackers are unable to analyse air traffic partners

Increasing digitalisation requires a shift towards cyber-resilient operational platforms

The focus of security has shifted towards ensuring the absolute authenticity of communication

ED-201 on Aeronautical Information System Security. These standards have become the essential common ground for security, providing a clear, verifiable benchmark for information security management that ensures every link in the communication chain is hardened against modern threats.

In Europe, this industrial baseline is being enforced through the NIS2 Directive, which classifies air traffic management as an 'essential infrastructure'. This shifts the landscape from voluntary guidelines to mandatory legal accountability, requiring providers to demonstrate resilience through thorough supply chain audits and rapid incident reporting. Within the European context, we also align with the EU Cyber Resilience Act (CRA) by utilising our 'Trusted-Zone Security' architecture. This approach ensures that every component in the voice chain is independently verified and documented, providing air traffic service providers with the transparent, resilient foundation they need to meet strict operational requirements. It is worth noting, however, that while compliance with the EU Cyber Resilience Act strengthens product level cybersecurity, in aviation the practical benchmark is set by EASA's safety driven view, where cyber resilience of ATM voice communication is inseparable from operational safety.

The United States Federal Aviation Administration (FAA) is navigating a similar path. Its regulatory focus is on the move away from traditional analogue infrastructure, ensuring the new National Airspace System is built on the 'Zero Trust' architecture, where every voice transmission must be verified. Our security approach follows Zero Trust principles, implemented through clearly defined trusted zones, resulting in a cyber resilient operational platform for mission-critical voice communication.

This aligns with standards from NIST (the National Institute of Standards and Technology), the US agency defining the specific cybersecurity frameworks used to protect critical infrastructure to prevent unauthorised access to flight-deck communications.

Asia Pacific also presents a high-growth regulatory environment. For instance, in a high-traffic hub like Singapore, the Cybersecurity Act mandates that Critical Information Infrastructure (CII) undergoes tough, recurring audits to maintain national safety.

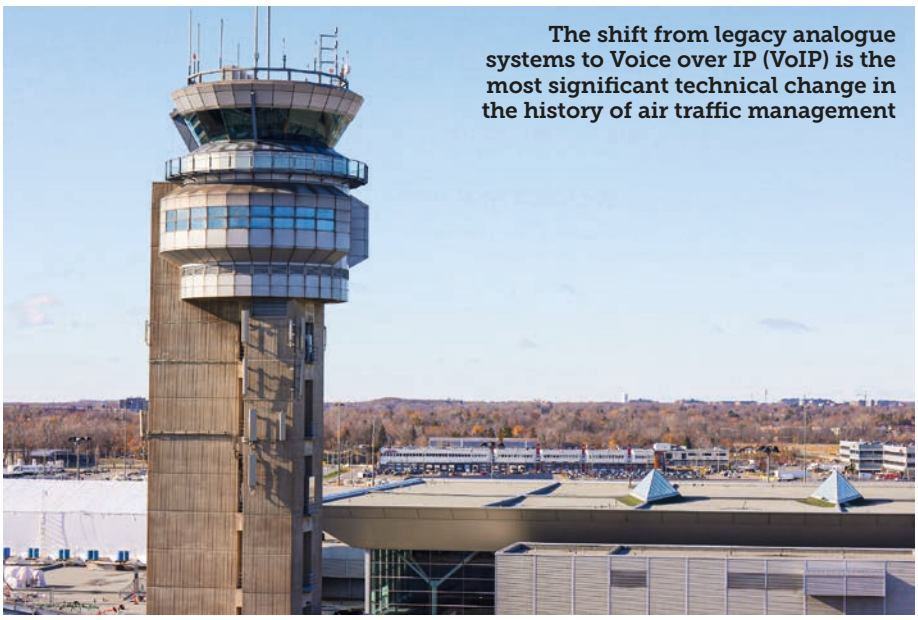
Essential infrastructure

The priority of voice security has shifted from being a technical requirement to a foundational pillar of modern aviation. In 2026, air traffic management is about protecting a critical national asset. For instance, in Europe, the NIS2 Directive elevates ATM to the status of essential infrastructure, on a par with critical services such as electricity and water.

We are seeing this play out very clearly in regional regulations. For instance, in Europe, the NIS2 Directive has legally reclassified ATM as 'essential infrastructure', placing it on the same security level as the power grid or water supply. This means security is not a choice, but a legal mandate.

By following global benchmarks like ISO/IEC 27001, the industry is creating a common shield against voice security threats, ensuring that ATM remains consistent and secure even when a flight crosses multiple national jurisdictions.

At the end of the day, whether it's a pilot or a controller, they need to know that the voice on the other end is authentic and uninterrupted, regardless of what is happening on the global political stage. Our goal is to ensure that technology remains a silent, secure partner in keeping the skies safe. AI



The shift from legacy analogue systems to Voice over IP (VoIP) is the most significant technical change in the history of air traffic management