A King Air 200 equipped with ClearVision. Image: Universal Avionics

Painting a picture

While the traditional facets of aviation safety remain, new technologies are helping crews fly safer or as safely in challenging conditions. Yet at the same time technological development brings its own safety challenges, as Paul Eden discovers.

Safety ought to be the constant underpinning all commercial aircraft operations. The fundamentals – observation, communication and quality maintenance among them – remain as they always have, while continued development in avionics and connectivity are facilitating new safety systems that support pilots in their fundamental safety tasks and bring new tools into the cockpit.

The definition of safety is evolving as aircraft and airport systems have increasingly become digital. Anyone stuck on the ground during the recent cyberattack on several European airports, or awaiting delivery of a new Land Rover, will appreciate the importance of cybersecurity.

Inconvenience and expense have so far been the primary outcomes of cyberattacks in the aviation space, but it would not do to assume that a future event will not threaten safety of flight.

For airlines generating ancillary revenues through onboard transactions, there is another threat – if not to the safety of flight, then the safety of profit margins.

Fraudulent card transactions have cost carriers dear in recent years, a penalty quickly offset by installing low bandwidth connectivity sufficient to process card payments in real time.

INFORMATION OVERLOAD

Situational awareness is key to aviation safety – from seeing and avoiding other traffic, through to risk management and avoiding weather hazards. Multiple systems have evolved using onboard sensors and external data streams to gather information from a variety of sources and deliver it as imagery and text into the cockpit.

The result is potentially better situational awareness and therefore improved safety, but there is a risk that this abundance of information might overwhelm crews.

Fighter pilots are familiar with the dangers of information saturation – they call the resulting confusion a “helmet fire”.

Manufactures of commercial aircraft avionics are working hard to bring the concept of sensor fusion – where a fighter’s mission avionics suite takes multiple data streams and “fuses” them into a coherent picture – to airliner and business jet cockpits.

A Boeing 737NG pilot wears the SkyLens product associated with the ClearVision system from Universal Avionics. Image: Universal Avionics

Among them, Universal Avionics has developed ClearVision, an enhanced flight vision system already in service with an airline operating ATR 72-600 turboprops.

Universal Avionics' CEO, Dror Yahav, says: "Its reliability and contribution to operational efficiency are tangible, bringing significant benefits especially when operating in low-visibility areas."

He adds: "We also have certification for Boeing 737NG models, and while we don't yet have an airline operator, we expect to introduce one in 2026 – the result of many ongoing discussions with potential 737 launch customers."

Universal Avionics has engineered ClearVision for installation across the commercial aircraft spectrum using the same core subsystems: a computer unit, software applications and multispectral camera.

The more capable and slightly larger EVS-5000 camera is available for airliners and business jets, while helicopters take the EVS-4000. Both cameras can detect LED runway lights in low visibility.

According to Yahav, the most significant difference between applications is in how pilots receive the video and overlain data.

He says: "On business jets we install a fixed, wide field of view head-up display, while for our airline customers we provide the SkyLens head-wearable display, which provides a 360-degree field of view and additional functionality. Helicopter customers take the SkyVis helmet-mounted display, which also allows night-vision goggle functionality."

ADS-B In data is presented only on the SkyLens and SkyVis devices, since the traffic it identifies is frequently outside the head-up display view.

In effect, a pilot employing either wearable solution can look at any piece of visible sky and see aircraft tagged and tracked by their ADS-B In signature – the effect is similar to that of a gamer tag in a video game.

ClearVision delivers a step up in situational awareness – so much so that while Universal Avionics expected pilots to wear SkyLens from take-off to top of climb and from initial descent to landing, many use it throughout the flight.

It is during landing in low visibility that the system really earns its spurs, however.

> "We also have certification for Boeing 737NG models, and while we don't yet have an airline operator, we expect to introduce one in 2026 – the result of many ongoing discussions with potential 737 launch customers."
>
> **Dror Yahav, CEO, Universal Avionics**

One of Gogo's network operations centres. Working through enhanced security packages and customer training, artificial intelligence is seen as both a threat and a defensive tool. Image: Gogo

Airports are increasingly replacing traditional runway lights with energy-saving low-maintenance LED units, but these have so small an infra-red signature that traditional IR-based enhanced vision systems struggle to see them in thick fog, heavy rain, snow or smoke.

As mentioned, however, the multispectral cameras feeding ClearVision pick up LED lights, displaying them as part of its 3D synthetic vision image.

'BAD ACTORS'

Cybersecurity is now an essential provision ensuring the integrity of aircraft systems, airport infrastructure and operator and passenger data.

Any aircraft connected to the internet is vulnerable to cyberattack – a fact some operators are slow to recognise.

A leader in business aviation, VVIP and government/defence connectivity, Gogo enforces a robust cyber defence strategy, working not only through its network operations centres but also through enhanced security packages and customer training.

Gogo company data reveals the frightening extent of cyberattack activity. Its cybersecurity prevents around 10,000 malware attacks on customer assets daily – and the company's cybersecurity experts keenly emphasise the potential of artificial intelligence (AI) as both a threat and a defensive tool, plus the importance of keeping secure the aircraft and sensitive data moved on and off it through whatever connectivity "pipe" is employed.

AI is enabling what Gogo refers to as "bad actors" to create convincing emails and voice messages that can tempt the unwary into interactions with chatbots posing as legitimate correspondents.

Account must also be taken of AI's ability to quickly and accurately cross-reference information across data sources including flight logs, passenger manifests, social media accounts and other locations, fuelling the creation of complex threats.

And since it never rests, AI can be tasked with launching multiple, large-scale attacks against complete systems and organisations, potentially invading flight management systems, communications networks and ground infrastructure – and, worryingly, using its persistence to break passwords.

On the flipside, AI can detect threats early for a rapid response, while behavioural analytics is a useful tool for detecting data anomalies.

Combined with its human cybersecurity experts, Gogo says it is using AI to create powerful defence mechanisms.

Within its cybersecurity offer, the company offers three levels of service – of which even the entry level delivers active threat monitoring, identifies discrepancies and initiates remedial activity.

The second level employs proprietary technology to "optimise a secure, accelerated tunnel through which encrypted, anonymised data passes from the aircraft to the ground and back", while the third creates a private cabin network from which data never reaches the public internet.

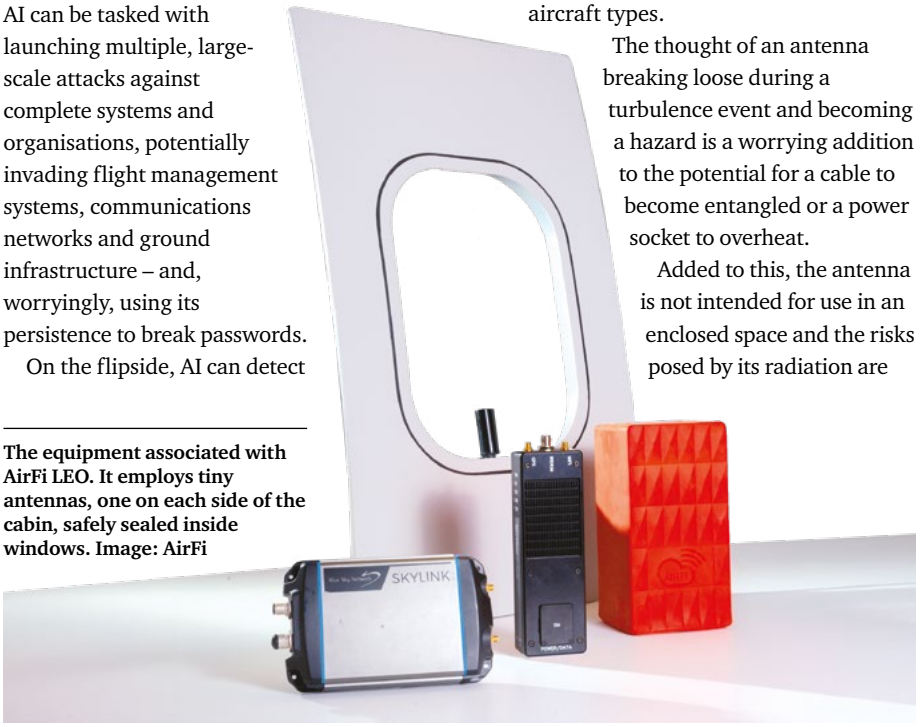
Connectivity powers many modern safety enhancements, but in one very specific example also appears to be presenting a potential risk.

Starlink has taken the commercial and business aviation markets by storm with its dedicated aircraft product, but anecdotal tales are emerging of operators using the same company's Mini system to gain low-cost in-flight connection.

Starlink does not promote Mini as an aviation platform, but the antennas are appearing in the cabins and cockpits of general aviation and smaller business aircraft types.

The thought of an antenna breaking loose during a turbulence event and becoming a hazard is a worrying addition to the potential for a cable to become entangled or a power socket to overheat.

Added to this, the antenna is not intended for use in an enclosed space and the risks posed by its radiation are



The equipment associated with AirFi LEO. It employs tiny antennas, one on each side of the cabin, safely sealed inside windows. Image: AirFi

> We deliver a dynamic picture of the aviation risk environment and an ability to look forward. We gather data and provide an analytical, operational overlay for airlines and, most importantly, explain what we think is likely to happen.
>
> **Andrew Nicholson, CEO and co-founder, Osprey Aviation Solutions**

not well understood. It is worth noting that all satcom antennas are powerful transceivers and the levels of electromagnetic radiation they receive and transmit are carefully specified, and their health risk defined.

PROTECTING REVENUE

Connectivity facilitates the AirFi LEO product, which offers basic passenger connection while enabling airlines to verify card transactions in flight with no need for larger satcom systems.

Rohit Malaviya, VP of Technology at AirFi, tells *Inflight*: "Onboard payment fraud is a significant concern for airlines, as traditional offline systems often cannot verify transactions in real time. It has been reported that 2 to 10 per cent of revenue can be lost due to fraudulent practices.

"The AirFi LEO system addresses this by providing a secure, always-on satellite connection that enables immediate online transaction validation directly with banking networks, ensuring fraudulent cards are detected before a sale is completed.

"Beyond real-time authorisation, AirFi employs a layered defence strategy, including end-to-end encryption, active tracking and blocking of blacklisted cards and other industry safeguards."

While AirFi LEO helps keep airlines safe from fraudulent transactions, its careful design also keeps other aircraft systems safe.

Malaviya says: "Operating within Iridium's certified aviation band and under strict power limits, the system ensures there is no interference with cockpit avionics.

"The AirFi LEO system was also built with a security-first architecture to safeguard airlines and passengers against malicious attacks. It is fully isolated from critical avionics networks, ensuring that no AirFi traffic can ever access or interfere with cockpit or aircraft control systems.

"Third-party applications like WhatsApp, Facebook Messenger and X run on passengers' devices which handle their own security, whereas AirFi internal applications have end-to-end encryption applied to all data and strict firewalls to prevent unauthorised access.

"In line with industry best practices and EASA/FAA cybersecurity guidelines, AirFi maintains a layered defence approach that combines network segregation, encryption, intrusion attempt reporting and regular security audits, hence guaranteeing that the benefits of in-flight connectivity are delivered without compromising safety or security."

BESPOKE INTELLIGENCE

Setting aside AI, technology is making aviation safer while simultaneously presenting new threats.

Risk analysis is key to creating safe flight plans in this complex environment, and Osprey Aviation Solutions has garnered a reputation for the quality of the risk analysis products it creates for airline, business aviation, government and military operators.

Among recent technological threats, Osprey was among the first agencies to warn of GPS jamming and spoofing around conflict zones – a threat causing problems for airliners in the Baltic states and other regions.

Osprey's CEO and co-founder, Andrew Nicholson, says: "We deliver a dynamic picture of the aviation risk environment and an ability to look forward. We gather data and provide an analytical, operational overlay for airlines and, most importantly, explain what we think is likely to happen.

"Then we consume risk and operational data, including flight plans and ADS-B data, to make output specific to a network or operator, so they can see which flights might be affected by changes in the risk environment.

"These products feed into our risk management tools, which support organisations as they work through their own risk management processes."

Fundamentally, Osprey provides bespoke intelligence products that enable airlines to plan safer or continuing safe operations as conflict, geopolitical and other risks evolve.

While interfering with GPS signals is a use of technology contrary to safe practice, the burgeoning possibilities offered by the latest computing techniques and AI are paying dividends elsewhere.

Universal Avionics, for example, expects to certify its Aperture system first for business aviation, where it will build upon the existing capability of ClearVision.

Yahav says: "It will enhance situational awareness by fusing data from sensors, cameras and avionics systems to display intuitive visual guidance, including runway obstructions, taxi routes, tagged traffic and much more.

"Alongside a massive effort to finalise its development and launch it to the market, we are making significant progress with hardware design, software development, AI training and certification, while adding more sensors and data inputs to enhance its performance." ■