Protecting the Connected Air Transport System



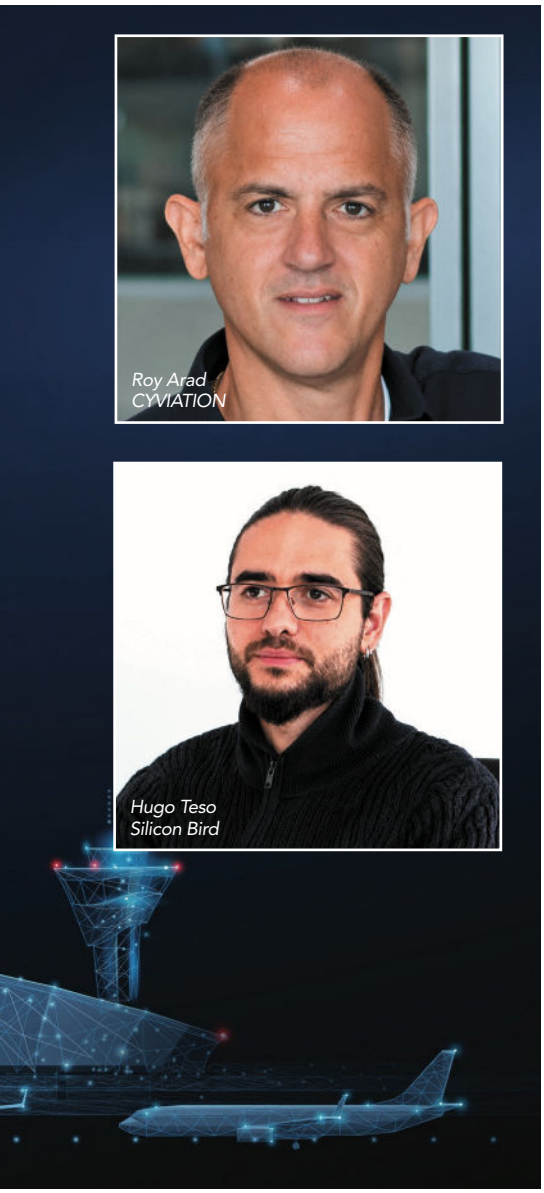
As commercial aviation becomes ever more connected, its exposure to cyberattacks extends beyond corporate networks to the aircraft, ground handlers, and flight deck systems. To examine the vulnerabilities across this connected ecosystem — and how the aviation industry can build true operational resilience — Transportation Security International convened a virtual roundtable of experts.

Our experts are:

Roy Arad, CYVIATION's chief revenue officer. Headquartered in New York, CYVIATION is a cybersecurity company dedicated to securing the aircraft itself. Through its SkyRay platform, the company builds a digital twin of each aircraft to remotely assess its systems, devices, and connectivity for vulnerabilities without affecting airworthiness, to give airlines and fleet operators continuous cyber threat intelligence and compliance monitoring.

Hugo Teso, Silicon Bird's CEO and founder. Silicon Bird is a European technology company focused on cybersecurity for complex cyber-physical systems across air, sea, and land. Using a proprietary virtualization platform that creates realistic, hardware-independent models of an aircraft's onboard electronics, data buses, datalinks, and networks, Silicon Bird allows airlines, MROs, manufacturers, and authorities to assess, test, certify, and train without taking physical aircraft out of service.

Transportation Security International: The modern air transport system is deeply interconnected, encompassing airlines, airports, air traffic management, cargo, ground handling, maintenance, communications, and the aircraft themselves. In this environment, what specific parameters



and vulnerabilities must be monitored most closely?

Roy Arad: I would start with something most people do not realize. There are almost no published vulnerabilities for aircraft. In IT, a security team gets a steady feed of known weaknesses to track and patch. For the airplane, that feed barely exists.

So, in a way, operators are blind today. It is not that they are ignoring the aircraft, it is that there is very little for them to monitor.

That does not mean the risk is not there. A modern aircraft takes in data from the ground constantly: navigation databases, performance data, EFB content, loadable software. Maintenance laptops and data loaders connect straight into it, and some of those laptops still run old, unsupported operating systems.

In my view maintenance tooling is one of the weakest links we have. On top of that, the aircraft depends on a lot of data it cannot check for itself: ADS-B, ACARS, NOTAMs, ATIS, weather, approach data and ground-based nav aids like VOR and ILS. So the things I would watch most closely are: exactly what software and configuration is on each tail, and what changed; the integrity of everything loaded onto the aircraft; who and what has access to it, physically and digitally, including EFBs, maintenance connections and wireless networks in the cabin; and the integrity of the navigation and operational data the crew relies on along the routes you fly.

If an operator cannot quickly answer, "what is on that aircraft and what changed," that is not an IT gap. It is a safety gap. That is what we help with. SkyRay gives operators the visibility the public record does not, by showing what actually applies to their own tails, and our Intelligence Operation watches the data aircraft depend on so operators are not left to find problems by chance.

Hugo Teso: I would point to three areas. The first is the boundaries between systems and between areas of responsibility. Aviation is a system-of-systems, and the seams between an airline's IT, ground infrastructure, data services and the aircraft are where ownership blurs. Attackers look for exactly that kind of seam.

The second is legacy technology. With new aircraft deliveries constrained, operators are extending the life of existing fleets and systems to keep them operational and revenue-generating. Those systems were designed for a different threat era, and every update that keeps them flying adds connectivity to foundations that were never built to be secure.

The third, and perhaps the most dangerous, is complacency. The industry risks becoming comfortable with paper-focused cybersecurity: compliance documents, risk registers and assessments that satisfy an audit. Meanwhile the real, technical challenges keep growing.

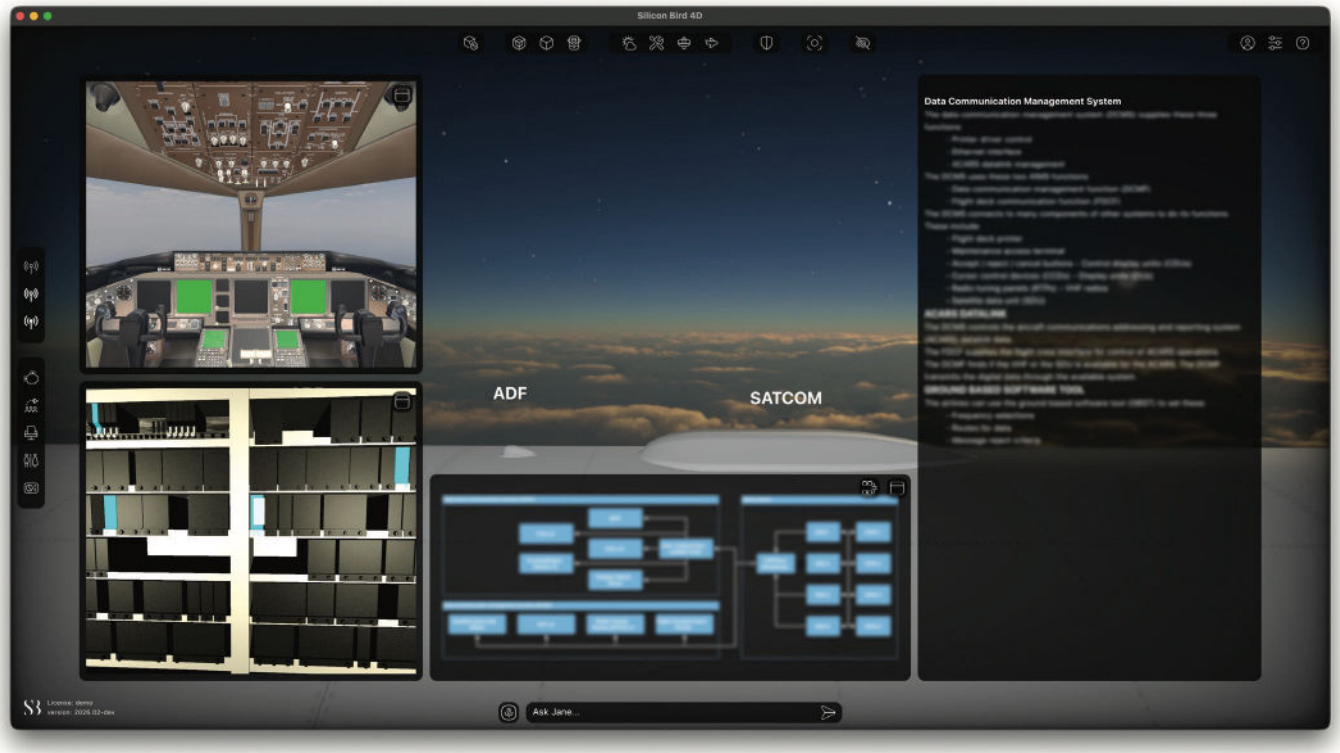
Transportation Security International: How wide-ranging is the threat landscape across the connected aircraft ecosystem, and what are the potential cascading impacts of a localized breach?

Teso: The exposed attack surface is so complex that no stakeholder has a single pane of glass covering all of it. As a result, the consequences of a localized breach are often impossible to predict on paper.

Consider a plausible scenario. A data load, such as a navigation database or software update, is corrupted at its source. It passes through the normal distribution chain and is deployed across many operators before anyone notices. It may have no safety impact at all, yet the operational impact could be significant: aircraft held on the ground, loads to re-verify, schedules disrupted across multiple airlines at once. A single point of compromise becomes a fleet-wide, multi-operator problem.

Arad: It is about as wide as the industry itself, because nobody operates alone. An airline depends on OEMs, MROs, software vendors, avionics suppliers, connectivity providers, ground handlers and airports. Every one of those relationships is an access path, and the security perimeter today runs far beyond the cockpit door.

On the ground, one supplier can take down many operators at once. On the aircraft side, the picture is different and in some ways more worrying. A lot of onboard data links were designed decades ago, when the physical wire was the security. ARINC 429, for example, dates from 1977 and has no message authentication. So bad data introduced on the ground can travel into the aircraft, and the crew may be the first and only ones to notice. That is the real cascade I think about. A breach that starts as an IT problem in a hangar or a vendor's system can end up in the cockpit as a safety problem.



Airlines, manufacturers, MROs and civil transport operators must demonstrate cybersecurity without disrupting the operation that pays for it. Silicon Bird's virtualization technology lets engineering and security teams work against representative onboard systems, so assessment and certification preparation do not depend entirely on scarce physical test assets. Silicon Bird image.

Transportation Security International: Can you point to specific incidents in recent years that best illustrate the severity of aviation cyber threats, and how were those situations managed?

Teso: GNSS spoofing is the clearest example. Interference with satellite navigation has moved from theoretical concern to daily operational reality, particularly around conflict zones.

According to IATA's flight data, GPS signal loss events rose by 220% between 2021 and 2024. Spoofing is the more insidious form: rather than blocking the signal, it feeds the aircraft false but plausible position data.

The response has been extensive in studies, workshops, safety bulletins, NOTAMs, crew procedures and, more recently, a joint EASA–IATA mitigation plan. All of this is valuable. But note what it largely consists of: managing the symptom operationally while trusting the robustness of the wider system to absorb the problem. The underlying weakness, receivers that can't reliably distinguish genuine signals from false ones, has been identified for years, yet a fix at the avionics level remains a long-term prospect. That's the lesson. Aviation is very good at studying a vulnerability and building procedures around it. It's far slower at actually removing it.

Arad: A few stand out for me. In September 2025, ransomware hit Collins Aerospace's MUSE check-in and boarding software. Heathrow, Brussels and Berlin were among the airports that had to fall back to manual check-in, and the EU cybersecurity agency ENISA confirmed it was a third-party ransomware attack. One supplier, many airports.

In August 2024, the Port of Seattle was hit by Rhysida ransomware, which disrupted ticketing, check-in, baggage and Wi-Fi at Sea-Tac. The Port isolated its systems, refused to pay and ran on manual processes while it rebuilt.

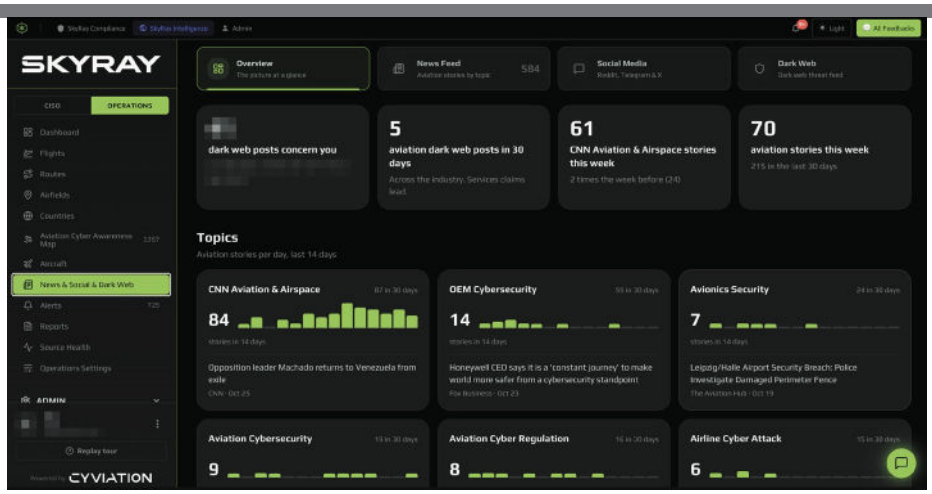
Navigation interference has moved even closer to the flight deck. In spring 2024, Finnair suspended its Tartu flights for about a month after GPS interference stopped aircraft from landing, until a ground-based alternative to the GPS approach was put in place. Crews across several regions now deal with jamming and spoofing as a routine part of the job.

More recently, in August 2026, a fake WiFi network called "Delta Wifi Fast" appeared on a Delta flight from Las Vegas to Atlanta. The crew spotted it, alerted the company and shut off WiFi for about 30 minutes. Delta said flight safety was never in question, and I believe that. But it was detected because a person happened to notice, not because a system did.

The same month, university researchers showed on a testbed built from real airliner components that a coin-sized device plugged into a maintenance port in the nose equipment bay could alter flight plan and weight and balance data in under 60 seconds. It was a lab demonstration, and the manufacturer said existing protections limit the real-world risk, but it makes the point that the aircraft itself is part of the attack surface.

Transportation Security International: What tools and methodologies are currently available to tackle these risks, and how do your organization's specific solutions fit into that toolkit?

Arad: The industry has good building



CYVIATION says SkyRay transforms aviation cyber intelligence from fragmented signals into continuous, operational threat visibility and control. SkyRay aims to give operators real-time awareness of threats to aircraft, routes and navigation systems. CYVIATION image.

blocks: airworthiness security standards like DO-326A, regulation like EASA Part-IS, threat frameworks, and threat intelligence sharing. The missing piece has been the aircraft. You cannot pen test an airframe in service the way you test a corporate network without putting its airworthiness at risk, so it simply is not done, and documentation ends up standing in for real evidence.

That is where we come in. SkyRay models each aircraft's systems and communication paths in a digital twin, so we can do on the twin what you cannot do on the airplane: test, map exposure, and answer the question that matters to an operator, which is not, "Does this vulnerability exist?" but, "Does it affect our aircraft?" We do it without any physical contact with the aircraft. We map that against AV-ATT&CK, our aviation extension of the MITRE ATT&CK approach, which covers 43 techniques across 13 tactics.

The other side is operational. People still talk about GNSS spoofing as the big story, but to me it is really yesterday's problem. What it proved is how cheap, easy-to-get tools can be used to feed false data to an aircraft. The same idea applies to ADS-B, NOTAMs, ACARS, ATIS, approach data, weather, VOR, ILS and more, all of which affect navigation and safety. Our SkyRay Intelligence Operation monitors all of these, so operations teams see when the data their aircraft depend on is being tampered with, not just the GPS signal. GPS Sentinel is part of that picture. SkyRay is offered as Compliance, Intelligence CISO and Intelligence Operation.

Our research team also finds and discloses vulnerabilities. This year we





Shown here is the SkyRay activity dashboard monitoring GNSS activity. Cyviation image

disclosed CVE-2026-1579 in PX4 Autopilot, flight-control software used on a large number of drones, where the command channel accepted unsigned commands by default. CISA issued an advisory on it with a 9.8 severity score. That kind of finding is why we applied to become a CNA.

Teso: The toolkit is maturing: risk assessment and threat modeling methodologies, security standards for airworthiness and organizations, information security management systems, monitoring, and technical testing on lab benches and test aircraft.

The problem isn't the absence of methods. It's access. Real, technical aircraft cybersecurity has traditionally required the aircraft itself, or expensive integration rigs, and those sit almost exclusively with manufacturers. Operational, legal and economic constraints keep everyone else out. An airline can't easily take an aircraft out of service for testing. A supplier rarely has the full system context its component lives in. An MRO may have no testing environment at all. Yet all of them carry cyber risk and responsibility across the aircraft's lifecycle.

This is where our approach fits. By virtualizing the aircraft's onboard systems, we aim to democratize access to the aircraft for cyber operations: assessment, testing, certification evidence and training. That access extends across the entire supply chain, not just to the manufacturer. It turns paper exercises into real, repeatable technical work.

Transportation Security International: Looking at the industry as a whole, what tangible steps have been taken to date to effectively fortify the sector against cyberattacks?

Teso: The regulatory foundations are now in place, and that's real progress. In Europe, Part-IS is the most significant step. Depending on the entity, it applies from October 16, 2025, or February 22, 2026, and covers maintenance organizations, air operators and air navigation service providers, among others.

Alongside it, the EUROCAE airworthiness security standards, the ED-202A, ED-203A and ED-204A family, give the industry a recognized framework for securing aircraft across design, certification and continued operation. Yet there is a risk in how Part-IS is perceived. It is often read simply as a requirement to put an information security management system in place. That interpretation leaves the door open for organizations to comply on paper while avoiding real, technical engagement with the security of the aircraft itself. Management systems are necessary, but they aren't sufficient. The regulation's intent is to treat information security as part of aviation safety, and safety ultimately lives in the aircraft. The next step is to make sure compliance translates into deep, technical aircraft cybersecurity across every organization that touches it.

Arad: After 9/11 the industry did the right things for that era: reinforced cockpit doors, much stronger screening, better physical security. Those measures worked and still matter. They were just built for a different threat.

The big change now is that regulators are treating cyber as a safety issue. EASA Part-IS is the clearest example. It started applying to design and production organizations and aerodromes in October 2025, and to operators, maintenance organizations, CAMOs and air navigation service providers in February 2026.

In the U.S., the FAA proposed rules in August 2024 that would require new transport category aircraft, engines and propellers to address intentional unauthorized electronic interactions. DO-326A has made airworthiness security part of certification for new designs. Information sharing has also improved, and more operators now report interference so others can learn from it.

The gap is the in-service fleet. Aircraft stay in service for decades while threats and rules keep changing, and too many organizations still treat cyber as a point-in-time compliance exercise rather than something you watch every day.

Transportation Security International: How are AI and other emerging technologies compounding the complexity of aviation cybersecurity?

Arad: AI lowers the bar for attackers. You can ask it almost anything, and I would bet some people are asking it how inflight entertainment and cabin networks work.

Most of what we see on commercial aircraft today is closer to pranksters testing what they can affect than people trying to bring an airplane down, but AI makes those people more capable very quickly. It also makes phishing aimed at crews and maintenance staff much more convincing. Our chairman, Arik Arad, has also warned that AI could eventually let attackers go after many aircraft at the same time instead of one.

At the same time, aircraft keep getting more connected: more WiFi in the cabin, more wireless data loading, more data flowing between the aircraft and the ground. Every new link is useful and every new link is another path in. Radio signals do not respect the security boundaries we draw inside an aircraft, which is exactly what the Delta WiFi case showed. The good news is that AI helps defenders too, especially with spotting patterns humans miss, like small anomalies in navigation and operational data or unusual activity around a specific tail.

Teso: The most important impact of AI, in my view, is that it lowers the barrier of entry into aviation. Historically, aviation technology was protected in part by

its specialization. Its protocols, data formats, architectures and documentation demanded years of domain expertise. A skilled cybersecurity professional from another field faced a steep learning curve before becoming effective against avionics.

AI collapses that curve. It can help someone interpret specialist technical documentation, understand unfamiliar protocols, analyze firmware and reason about system architectures far faster than before. In practice, this means cybersecurity expertise built in other sectors can now be transferred into the aviation ecosystem with much less effort.

The consequence is clear: security through obscurity no longer works. For years, the complexity and closed nature of aviation technology acted as an informal defense. That defense is eroding quickly. The industry must assume that the attackers of tomorrow understand its systems as well as it does and design its security accordingly.

Transportation Security International: What is on the horizon regarding the next generation of both cyber threats and threat mitigation strategies?

Teso: The economics of attacking aviation are changing. Historically, a real cyberattack against an aircraft was far more expensive and demanding than traditional physical attacks such as a hijacking. It required rare expertise, specialized equipment and access to the target technology. That cost was, in effect, a protective barrier.

With the arrival of AI, that barrier is falling. We should expect aviation cyberattacks to become more common and eventually commoditized: capabilities that once required a well-resourced team becoming packaged, repeatable and available to far less sophisticated actors.

On the mitigation side, the answer is to use the same tools to stay ahead. If attackers use AI to accelerate their understanding of aviation systems, defenders must use it to accelerate testing, discovery and remediation, at a scale and pace that manual, paper-based approaches can't match. Combined with realistic virtual environments, AI-driven security testing can explore systems continuously. That means finding weaknesses before adversaries do, not after an incident forces the issue.

Arad: On the threat side, I expect more attacks through suppliers and maintenance, because one compromise there reaches many aircraft. I expect more blending of physical and cyber, where someone with brief, trusted access to an aircraft introduces something digital. And I expect the cheap tools that made GNSS spoofing possible to be turned on the other data aircraft rely on, from ADS-B and ACARS to weather, approach data and nav aids.

On the mitigation side, the direction has to be treating the aircraft as a monitored asset, not a sealed box. That means knowing the exact configuration of every tail, verifying what gets loaded onto it, watching the integrity of the data it depends on, giving crews the tools and procedures to detect things like rogue networks systematically instead of by chance, and tailoring threat intelligence to the specific aircraft an operator flies. Vulnerability disclosure will mature too, with clearer paths for reporting and fixing weaknesses in aviation products. Above all, security has to become a continuous discipline, not an annual audit. TSI

By virtualizing the aircraft's onboard systems, Silicon Bird says it aims to democratize access to the aircraft for cyber operations: assessment, testing, certification evidence and training. That access extends across the entire supply chain, not just to the manufacturer. Silicon Bird image.

