On-board Internet for Flight Inspection Aircraft

Dr. Mirko Stanisak

System Engineer & Research Manager
Aerodata AG
Braunschweig, Germany
Phone: +49 531 2359-304
E-mail: mirko.stanisak@aerodata.de

Paul Frost

Software Engineer
Aerodata AG
Braunschweig, Germany
Phone: +49 531 2359-175
E-mail: paul.frost@aerodata.de

ABSTRACT

Various office work tasks nowadays require Internet connectivity - from online cloud storage via online meetings to online web services. On commercial jetliners, online connectivity has improved significantly in recent years, allowing office-like Internet use even during oceanic cruise flight.

Flight inspection systems installed on specifically modified aircraft could be considered offline for the last decades. This has been changed lately by the availability of connectivity options for these types of aircraft, which allows for certain online workflows even during flight inspection missions.

This paper will detail possible Internet connectivity options specifically for flight inspection purposes, along with their respective pros and cons. Based on this, various possible use cases will be identified and analyzed – ranging from receiving GNSS reference station data to synchronization of flight inspection measurements and results.

From a cyber security standpoint, onboard Internet connectivity poses an additional attack vector which needs to be addressed very carefully. This paper will explain the consequences and possible mitigations for ensuring safe, secure and reliable operations over the complete lifecycle of flight inspection aircraft.

INTRODUCTION

The ubiquity of Internet connectivity has lead to tremendous changes in work processes over the past few years. In office environments, hardly any process nowadays is offline, with cloud storage and online systems being used more and more intensively.

In the past, most aircraft had been offline, with no systems being connected to the Internet directly. In general, airborne Internet connectivity options have been available for several decades, although their limited overall performance and high expenses have prevented their use in flight inspection.

Over the last few years however, new technologies have emerged that have added completely new connectivity options for aviation users as well. With different characteristics and operational constraints, these systems can enable the use of the Internet in the flight inspection domain.

This paper will introduce the challenges of Internet connectivity from a cybersecurity standpoint first, including their corresponding requirements for official approval and the newly added threat vectors. Subsequently, different currently viable Internet connectivity options for small and medium aircraft will be introduced and compared. Based on these, different use cases in flight inspection will be identified and assessed thereafter, especially regarding their respective gain in operational efficiency.

CYBERSECURITY CHALLENGES

In the past, automatic flight inspection systems were considered non-essential equipment, not affecting the general aircraft functions in any way. Without additional connectivity options, the automatic flight inspection systems operated independently from the other systems.

Thus, from a cybersecurity perspective, the main threat that was considered was infected removable media (like SD cards or USB flash drives). Various mitigation measures were introduced to counter this threat and limit potential consequences.

When introducing new interfaces to an aircraft (e.g. by adding Internet connectivity as part of integrating an automatic flight inspection system), additional attack vectors become possible, which must be analyzed and mitigated.

Certification Requirements

Any modification of existing aircraft systems must be checked for cybersecurity aspects nowadays to ensure airworthiness. The exact guidelines for this depend on the approving authority and tend to change constantly. The key requirement here is to ensure that "intentional unauthorized electronic interaction" cannot adversely affect the aircraft's functions.

The European Union Aviation Safety Agency (EASA), for instance, includes cybersecurity guidance as part of their "General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances" (AMC-20) [1]. Here, AMC 20-42 requires that "any potential intentional unauthorised electronic interaction (IUEI) security threat and vulnerability that could result in an unsafe condition" [1] shall be assessed using a Product Information Security Risk Assessment (PISRA), which is a formal multi-step analysis framework based on ED-202A [2] and ED-203A [3].

First, the environment of the system (including interfaces and external factors like organizations or processes), the assets themselves, and possible attack paths need to be identified and collected. These lists are the basis for the next steps.

Then, the influence of every attack path needs to be mapped to every asset for a safety assessment of possible consequences. Subsequently, security mitigation actions must be considered or added until the resulting risk is acceptable.

The results of the PISRA affect not only the modification of the aircraft itself, but also possible future challenges to be addressed as part of the Instructions for Continued Airworthiness (ICA) (based on ED-204 [4]), e.g. installing potential future software updates in case of vulnerabilities.

Flight Inspection aircraft are usually operated with just crew on board. Local interactions can thus usually be mitigated by adequate training of the crew members. Remote interactions (e.g. via Internet connectivity) on the other hand need to be addressed and mitigated very carefully.

Network Separation

Legacy automatic flight inspection systems (AFIS) are connected via several isolated local area networks (LAN). These networks are either separated physically (different cables and switches) or logically (different IP addresses or VLANs). This ensures that all relevant data within the flight inspection system can be exchanged reliably.

If a network segment is connected as-is to the Internet, every component of this network could communicate with the Internet and could potentially also be attacked. Thus, for security and commercial reasons, all traffic to and from all components must be monitored and restricted as stringently as possible using a firewall appliance.

This firewall appliance incorporates routing and firewall functionalities. It serves as a central communication node between the flight inspection system and the Internet using (at least) two network interfaces for translating between different zones. The internal network is connected to the FIS network. The external network interface connects to the aircraft's connectivity solution for internet access. A typical network separation with an automatic flight inspection system is shown in Figure 1.

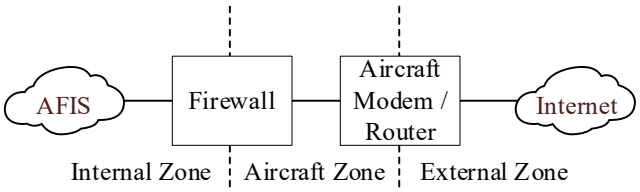

Figure 1: Physical Network Separation into Zones

For meeting the cyber security requirements, the firewall must restrict all in- and outgoing traffic as much as possible while still allowing the required services. As the services needing Internet connectivity (as detailed later in this paper) are different for each operator, the firewall must be highly configurable by the manufacturer of the flight inspection system, while also meeting the highest standards throughout its operational service life.

Central Data Repository

Most operators store their flight inspection data, results, and/or reports on a central data storage facility. This way, all relevant data is kept at a central facility and can be used for further assessments (e.g. for predicting navigation aids to leave tolerable limits).

Historically, the data taken by an automatic flight inspection system was transferred manually to these central data repositories via transportable storage media (like SD cards or USB flash drives) when at the home base. With the availability of Internet connectivity on the flight inspection aircraft, this transfer could happen via Internet instead, if the data repository can be accessed remotely for this purpose.

The flight inspection data represents critical commercial data and must be specifically secured, both for high availability of the service and the integrity of the data. From a cyber security perspective, it is important to protect the critical data from falling into the wrong hands and to protect it from being altered, while still being easily available to authorized users and processes.

This requires methods like backups at different locations, uninterruptable power supplies, emergency power generators, redundant Internet access lines, mandatory certificate-based authentication and mandatory encryption at all levels (e.g. via Virtual Private Networks).

AIRBORNE INTERNET CONNECTIVITY

Modern commercial transport aircraft often offer Internet connectivity for passengers, even in remote and oceanic areas. Internet connectivity is provided by different means, depending on factors like aircraft type, operator, and current location.

Smaller aircraft (like the ones typically used for flight inspections) face different challenges when integrating Internet connectivity than the usually larger transport-category aircraft. Despite the differences in size, operational envelope, and data rate requirements, the available connectivity options use the same backends for both categories of aircraft.

This section will introduce different Internet connectivity options and describe their modes of operation. In order to make use of these connectivity systems, an aircraft needs to integrate additional antenna systems (external) as well as corresponding modems (internal).

Satellite based systems operate in different frequency bands with distinct characteristics. The IEEE defines the relevant microwave bands as shown in Table 1.

Table 1: IEEE Microwave Band Definitions

Band	Frequency Range
L	1 - 2 GHz
S	2 - 4 GHz
C	4 - 8 GHz
X	8 - 12 GHz
Ku	12 - 18 GHz
K	18 - 27 GHz
Ka	27 - 40 GHz

The different frequency bands have different RF characteristics regarding available bandwidth, attenuation by precipitation, connection stability, free space loss and antenna technology. The satellite service providers use different frequency bands for optimizing their satellite's usability for specific situations.

L-Band services (between 1 and 2 GHz) are the most robust and reliable links, as precipitation does not notably interfere with RF signals. However, the available bandwidth (and thus the resulting maximum data rate) is limited. Subsequently, L-Band services are primarily used for safety-of-life applications, where stability is more important than the data rate. This is why most operational satellite communication (e.g. for CPDLC) happens via L-Band links. Aircraft modems and antennas are small and commonly used even on smaller aircraft.

RF signals at higher frequency bands (X, Ku, K, and Ka bands) are used when high data rates are required, e.g. for passenger connectivity. Compared with L-Band services, higher frequencies allow larger bandwidths to be used, but require more complex aircraft antenna systems. While gimbaled high-directivity antennas were used in the past, modern antenna systems use active electronically scanned array (AESA) antennas. These antennas are complex and integrate a high number of distinct elements, which are small individually, but sum up in total size.

All airborne Internet connectivity systems require additional antennas, located either on the top of the fuselage (e.g. for satellite communication) or on the bottom (e.g. for cellular communication). In addition, a connectivity modem (which usually also acts as a router and/or access point) must be installed in the cabin.

When installing any additional systems on an aircraft, it must be ensured that these systems do not interfere with any primary function of the aircraft. This implies numerous careful tests to be conducted before obtaining an approval of airworthiness. In addition (as stated before) cybersecurity risk assessments must be conducted when integrating new interfaces as part of an aircraft modification. For modifications of flight inspection aircraft, additional tests are needed to ensure that the measurement quality of the flight inspection system is not degraded in any way, too.

For comparing different connectivity options, the following parameters will be used:

- Data rate: The data rate specifies the speed of a connectivity technology, i.e. how much data can be transferred per unit of time. It is usually given in both data flow directions (uplink & downlink), as they can differ significantly. Depending on the actual data rate, it can be given in units like kB/s or MB/s. The achievable data rates depend on various

factors. The values given in this paper are approximations only.

- Latency: Communication latency originates from delays due to the round-trip time of data packets. The longer it takes a data packet to transfer between the user and its corresponding server, the more the user will be affected by the latency. For a complete request and response, all signals must travel from the user to the server and back again twice. The additional round-trip delay (Δt) depends on the distance (d) and the speed of light (c) in the specific medium:

$$\Delta t = \frac{4 \cdot d}{c} \qquad (1)$$

- Availability: Not all connectivity options are available everywhere. Some options have distinct service volumes in which a certain service is guaranteed, while others provide real global Internet connectivity.
- Integration: For airborne connectivity, an aircraft must incorporate at least a modem, a router and an antenna system. The complexity of the corresponding equipment varies significantly.
- Cost: Nowadays, most internet connectivity is billed according to a subscribed data plan. The resulting total expenses for internet traffic thus vary considerably.

In the next sections of this paper, different connection technologies and their respective characteristics will be compared using these parameters.

Geostationary Satellites

Geostationary satellites (like classical TV satellites) are placed in a specific orbit, at which the satellites move with a speed matching the rotational velocity of the Earth. This way, geostationary satellites appear at a constant elevation and azimuth for a stationary user. Due to their position overhead the Earth's equator, the relative elevation of a geostationary satellite reduces as the user's latitude increases. Thus, geostationary satellites are available globally, except for the polar regions.

In a geostationary orbit, satellites are d=35.786 km away from Earth's surface. According to equation (1), this results in an additional latency of almost 500 ms for a complete request and response. Communication via geostationary satellites thus always results in an additional latency compared to other methods. In addition, the rather low power levels (due to free-space loss) require more robust encoding schemes compared with other technologies, also limiting the achievable data rates.

Geostationary satellites are operated by different commercial service providers at various orbital positions. However, user contracts are usually not arranged with the satellite operators, but with intermediary companies selling connectivity plans for certain satellites. This results in a wide variety of costs, data volumes and data rates, depending on the subscription.

Various operators operate geostationary satellites at different longitudes and offer services to different users. Some GEO service providers are summarized in Table 2.

Table 2: Maximum Achievable Data Rates via GEO Satellites

System	Uplink (max)	Downlink (max)
Inmarsat / Viasat	400 kbps (L Band)	400 kbps (L Band)
	5 Mbps (Ka Band)	50 MBps (K Band)
Intelsat	3 Mbps (Ku Band)	25 Mbps (X/Ku Bands)

Due to the large distances between users and geostationary satellites, high-gain antennas must be used. While high-gain airborne L-band antenna installations are common along various types of aircraft, they can offer only modest data rates. Services with higher data rates use higher RF frequencies and require huge antennas to be integrated on top of the aircraft's fuselage. These systems can be predominantly found on large jetliners, but have never been used on flight inspection aircraft yet.

In summary, geostationary satellites are very convenient for achieving coverage in non-polar regions. The long distances between the satellites and the users result in low latencies and the need for high-gain directional antennas for reliable communication.

Low-Earth-Orbit Satellites (LEO)

Satellites in low earth orbits (LEO) are defined by an orbit height below 2,000 km and thus an orbital period of 128 minutes or less. At these altitudes, the atmospheric drag limits the lifespan of satellites. The shorter distances between the user and the satellite allow for lower transmit powers, smaller satellites and less communication delay. Due to their fast movement, multiple satellites with high-rate inter-satellite data links (e.g. via laser communication) are required to achieve true global availability of service.

In recent years, numerous service providers have started constructing LEO constellations. Most of them (like SpaceX Starlink, Eutelsat OneWeb or Amazon Kuiper) focus on high-speed Internet connectivity for remote (stationary) locations and operate at low orbit heights. Other constellations (like Iridium) operate at slightly higher altitudes and prioritize reliability and availability over high data rates for specialized communication services. Table 3 summarizes the achievable data rates of the different LEO connectivity services.

Table 3: Maximum Achievable Data Rates via LEO Satellites

System	Uplink (max)	Downlink (max)
Iridium	350 kbps (L Band)	700 kbps (L Band)
Starlink	60 Mbps (Ku Band)	220 Mbps (X/Ku Bands)
OneWeb	30 Mbps (Ku Band)	150 Mbps (X/Ku Bands)
Kuiper	100 Mbps (Ka Band)	400 Mbps (Ku/K Bands)

The high-rate LEO services tend to be especially less expensive per transferred data volume than the slower L-Band services. It must be noted that not all subscription plans intended for stationary ground use can also be used for airborne users. Some service providers restricted these contracts to certain maximum velocities and/or altitudes in favor of specialized (and more expensive) plans for aircraft users.

LEO satellites move at high relative velocities compared to its users, resulting in significant relative angular velocities and Doppler frequency shifts. While this is acceptable for the slower L-Band services, the faster LEO connectivity options (in the X/Ku/K/Ka bands) require active electronically scanned array antennas, which can switch over from one satellite to the next one without any noticeable service interruption. These AESA systems are complex, highly proprietary, and (due to the large number of individual antenna elements) rather large in size, which makes the integration into different types of aircraft challenging. While commercially approved installations are available for certain systems and aircraft types, they focus on transport category aircraft or larger business aviation aircraft.

Flight inspection aircraft are usually smaller and require significant areas on the fuselage for additional FIS antennas. Thus, bulky active antennas for high-rate Internet communication have not been integrated into a flight inspection aircraft yet. In contrast, antennas for L-Band services are smaller and have been integrated into flight inspection aircraft for years. At least some installations can switch transparently between GEO and LEO L-Band services (e.g. Inmarsat and Iridium) for a more reliable Internet connection.

In summary, connectivity services via LEO satellites are optimal when no specific service area can be defined. In contrast to GEO satellites, the Internet connectivity via LEO satellites always benefits from lower latencies. L-band services can be integrated easily but can provide modest data rates only. Higher data rates are technically possible using the modern LEO satellite constellations operating at higher RF frequencies, but require very complex antenna installations.

Cellular Connectivity

Cellular mobile networks have become omnipresent over the past decades in all populated areas. Next to voice services (telephony), cellular networks also allow for data communication. Over the years, the networks have incorporated numerous standards (e.g. UTMS, LTE, 5G) with different characteristics, maximum data rates, availability and latencies. User modems usually support multiple technologies for backwards compatibility.

Typical cellular mobile networks are neither designed nor intended to support airborne users for multiple reasons. The high relative velocities of aircraft can cause Doppler frequency shifts above the design limits and complicate the handover between different cells. High up in the air, an aircraft user is visible to multiple ground stations.

Most of these limitations are nowadays lifted by modern cellular modems specifically designed for aviation use. These systems, usually consisting of an antenna, a modem, and a router, are fully compliant with the relevant standards and allow for continuous data reception up to certain velocities and altitudes. As a rule of thumb, modern aviation cellular modems can be used with ground speeds of up to 250 knots and heights of up to 6,000 ft AGL. Typically, they are used on emergency medical helicopters for patient monitoring and communication with hospitals.

This makes such systems a very good fit for typical flight inspection aircraft, which tend to operate within these limits. The antennas (and modems) are rather compact, so that they can be integrated along with the other antennas installed as part of the flight inspection system.

Mobile communication standards (especially newer standards like 5G) allow for high data rates and low latencies. Their use requires a plan with one (or more) service providers via (embedded) subscriber identity modules (E-SIM/SIM), but usually include significant traffic allowances at minimal costs.

Wi-Fi (IEEE 802.11)

Wireless local area networks (WLAN) according to the IEEE 802.11 standards are currently the dominant technology for providing high-rate Internet connectivity. Wi-Fi connectivity can be used in two different ways in flight inspection aircraft.

On the one hand, Wi-Fi is often used by aircraft installations to provide passengers and crew with online connectivity. It must be ensured that a Wi-Fi installation does not interfere with the aircraft's primary functions. One example for guidance here is EASA's certification memorandum CM-ES-003 [5], which ensures that neither intentional nor unintentional RF emissions interfere with any of the aircraft's equipment.

On the other hand, flight inspection aircraft can also use Internet connectivity provided by ground infrastructure, e.g. within a hangar on the aircraft's home base. By connecting the flight inspection system to this Wi-Fi network, tasks like recording backup could be automated.

Comparison of Connectivity Options

Table 4 compares the key characteristics of the different connectivity options in a simple (yet subjective) qualitative way for a generic airborne user. This comparison might look different for specific applications or scenarios.

Table 4: Qualitative Comparison of Different Connectivity Options for General Airborne Users

	GEO		LEO			
	L-Band	Other Bands	L-Band	Other Bands	**Cellular**	**Wi-Fi**
Data Rate	☹	☺	😐	😀	😀	😀
Latency	😟	😟	☺	☺	😀	😀
Availability	😐	😐	😀	😀	☹	😟
Integration	☺	😐	☺	😐	☺	☺
Cost	☹	☹	😐	😐	😀	😀

Legend: 😟 very bad, ☹ bad, 😐 medium, ☺ good, 😀 very good

In flight inspections, the limited available fuselage space (due to numerous additional measurement antennas and rather small airframes) complicates the integration of high-rate satellite systems. L-band Internet connectivity via GEO or LEO satellites is present sometimes, but with limited data rates at high costs.

During missions, flight inspection aircraft spend significantly more time at low altitudes than in cruise, which is reciprocal to how most other aircraft are being operated. In addition, flight inspection aircraft mostly operate in the vicinity of airports, where cellular networks can be assumed to be available. Thus, integrating Internet connectivity into their aircraft via a cellular modem can be a good fit for many flight inspection operators. Such systems require only small external antennas but provide high-speed and low-cost Internet connectivity in the areas where flight inspection aircraft are typically operated. It just must be ensured that the cellular connectivity does not degrade the measurement performance or affects any primary aircraft function.

When on the ground, available Wi-Fi networks could be used via an external Wi-Fi antenna. This, for instance, could enable the automatic flight inspection system (AFIS) to perform high-volume data transfers when on the ground, potentially also using ground power.

To conclude, Internet connectivity can be integrated into flight inspection aircraft in different ways. The best connectivity option depends on the intended operation, the aircraft type, and the foreseen applications of Internet connectivity. Different possible applications (with different requirements) will be detailed in the next section.

APPLICATIONS IN FLIGHT INSPECTION

The previous chapter defined different technologies for providing general Internet connectivity to flight inspection aircraft. Using one or multiple of these technologies, the flight inspection system can now make use of this foundation for various applications. This list is not comprehensive, but just a list of potential interesting applications.

From a cyber security perspective (as stated before), all Internet connectivity needs to be constrained as far as possible. All Internet traffic not required for the intended applications should be blocked by a firewall.

High-Precision Reference Positioning

Flight inspection systems require a high-precision reference position. This usually is based on phase-differential GNSS (like PDGNSS or RTK), which requires GNSS data from a continuously operating reference station (CORS) at a known position on the ground.

For this GNSS reference data, temporary GNSS ground stations with a telemetry link have been used for decades. Setting up such a reference station, however, requires intermediate landings at the inspected airports. Instead, with Internet connectivity, it is now possible to obtain GNSS reference data from (commercial) networks of continuously operating reference stations (CORS), which are primarily being used e.g. for surveying applications [6].

Numerous networks for GNSS data are available globally, usually covering specific service areas. With Internet connectivity, flight inspection systems can obtain GNSS data this way and use the data for calculating a high-precision positioning reference, using principles like Phase-Differential GNSS (PDGNSS), Real-Time Kinematics (RTK) or Precise Point Positioning (PPP). The GNSS data is encoded very efficiently, so that the required data rate is rather limited.

E-Mail Communication

Sometimes, the measurements taken during a flight inspection are not as unambiguous as intended. Various effects can result in strange looking graphs and raise questions regarding the quality of a navigation aid. Often,

however, the operator of the flight inspection system must concentrate on the next measurements instead of performing a deep analysis of previous measurements while in the area.

In this case, Internet connectivity can be used to contact a dedicated expert (possibly at the operator's premises) for support via e-mail. The AFIS software supports this workflow by attaching plots, results, and other information to an e-mail. Once received, the expert can analyze the data for a fast recommendation, which can be sent back to the aircraft via e-mail.

As e-mail is a standardized and well-established means of communication, this does not impose any additional requirements on the expert's side and allows for faster and more efficient decisions.

Sharing of Measurements & Results

During the commissioning of a new ILS ground installation, the ground installation needs to be tuned according to the measurements taken by a flight inspection system. Having the detailed results from the flight inspection helps the ground technicians to set up all parameters as efficiently as possible.

For this use case, dedicated data downlink systems have been used in the past, incorporating a telemetry receiver and a specialized computer system with corresponding software.

With Internet connectivity on board (and on the ground), the Internet can be used to provide ground technicians with the detailed data as required. An additional telemetry system (with corresponding frequency approvals etc.) is no longer required in this case.

Virtual Private Network

Virtual Private Networks (VPN) are technologies for connecting networks with each other via insecure networks (like the Internet). VPNs are commonly used for connecting local company networks at remote locations or for integrating single clients (independent of their location) into a local area network (LAN).

To prevent a listener on the insecure network from decoding the data transferred via the VPN connection, a strong end-to-end encryption and user authentication is enforced, often complemented by multi-factor authentication. If implemented properly, VPNs play a vital role for secure communication within company networks.

In flight inspection aircraft with Internet connectivity, the integrated firewall can be configured to route all data via the operator's company VPN. This ensures direct and secure communication between the AFIS and servers on the company network. This allows the integration of the AFIS with company-internal services and processes. Details are however highly dependent on the respective organization and their requirements and constraints.

Synchronization of Recordings

All input data of an automatic flight inspection system is recorded continuously in a time-synchronized manner to allow its later post-processing. In addition, processed data like graphs, reports and analyses are often also included in this data recording. Subsequently, the file sizes of the resulting recordings are large.

Currently, all inspection recordings are physically transported to the operator's central data repository via transportable storage media (SD cards, USB flash drives, etc.). With the presence of high-rate and inexpensive internet connectivity (e.g. via cellular services or Wi-Fi at the hangar), this synchronization of new inspection data can be performed automatically through the Internet.

Various technical approaches exist for synchronizing local data with a central data repository. Algorithms like rsync ensure that the amount of transferred data is minimized, while new data is synchronized with the server automatically.

As mentioned before, this requires the central data repository to be accessible from the Internet. This central component must be included in the overall cybersecurity analysis to ensure that critical data is protected.

Online Geographic Data

Geographic information systems (GIS) are powerful tools for checking or analyzing geographical-bound data. Especially with dynamic map tiles displayed behind the data, these tools allow both preplanning and analysis of flight inspection missions.

With working and reliable airborne Internet connectivity, tools like Google Earth or QGIS can be used with various map backgrounds, even with volatile data (e.g. the current weather or temporary NOTAMS). This can increase the situational awareness of the FIS operator significantly, especially when altering the originally planned flight inspection procedures.

Remote / Autonomous Operation

Airborne Internet connectivity might also be an enabler for future reduced-crew flight inspection operations. Automatic flight inspection systems are usually controlled almost completely via software, without the operator needing to operate any hardware directly.

In addition, modern automatic flight inspection systems already support certain fully automatic measurement modes, which are intended to collect measurement data even on ferry flights without a FIS operator [7].

In the future, given continuous and reliable high-rate Internet connectivity, it might be possible technically to perform flight inspections without a dedicated FIS operator on board, but to assess the flight inspection measurements in real time from a centralized facility on the ground. Next to live and continuous date streaming, this would require additional means of communication between the FIS operators on the ground and the pilots on the aircraft. One possibility here might be to integrate voice-over-IP (VOIP) technology with the aircraft's intercom system.

CONCLUSIONS

Internet connectivity is becoming increasingly common and available in aircraft. Different connectivity options can be integrated to provide Internet access, with varying speed, availability and technologies. The specific choice depends on various factors like aircraft type, intended operation, and operational requirements.

When integrating connectivity technology into an aircraft, airworthiness is not only limited by the safety of the overall aircraft, but also by its security. These cybersecurity requirements include a detailed security risk assessment, which must include all connected components of an aircraft. It must be ensured that intentional unauthorized electronic interaction does not endanger the safety of the aircraft and its operation.

When integrating Internet connectivity in flight inspection aircraft, this leads to multiple challenges, which must be addressed. From a cybersecurity standpoint, the automatic flight inspection system (AFIS) is no longer an isolated system and therefore requires specific mitigation actions. The connectivity technology must be integrated into the aircraft, while ensuring that the crucial flight inspection measurement performance is not degraded.

Flight inspection operations differ significantly from other kinds of operations. With these constraints, other connection technologies might also be viable options next to satellite connectivity. Airborne cellular modems, in particular, require only small antennas and can provide fast, reliable and cost-efficient Internet access when operating at low altitudes in areas with cellular coverage. Due to this, cellular connectivity can be a very good fit for flight inspection aircraft and their typical operation.

Independent of the technology used, Internet connectivity can be used in flight inspections for various tasks, which have the potential to increase operational efficiency significantly. Thus, for future flight inspection operations, Internet connectivity should be seen as an enabler for even more connected processes and a higher general efficiency.

REFERENCES

[1] European Union Aviation Safety Agency (EASA), *"AMC-20: General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances"*, Amendment 23, January 2022

[2] European Organisation for Civil Aviation Equipment (EUROCAE), *"ED-202A: Airworthiness Security Process Specification"*, June 2014

[3] European Organisation for Civil Aviation Equipment (EUROCAE), *"ED-203A: Airworthiness Security Methods and Considerations"*, June 2018

[4] European Organisation for Civil Aviation Equipment (EUROCAE), *"ED-204: Information Security Guidance for Continuing Airworthiness"*, June 2014

[5] European Union Aviation Safety Agency (EASA), *"Certification Memorandum CM-ES-00: Guidance to Certify an Aircraft as PED tolerant"*, Issue 2, May 2024

[6] M. Stanisak, P. Frost, *"Efficient Flight Inspection Without Reference Station"*, Proceedings of the International Flight Inspection Symposium (IFIS) 2026, May 2026

[7] Marcel Hoffmeister, Stefan Jageniak, Andreas Kleffmann, *"Autonomous Data Collection"*, Proceedings of the International Flight Inspection Symposium (IFIS) 2026, May 2026