Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communication System (LDACS)

Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganell,
Daniel M. Mielke, Alexandra Filip-Dhaubhadel, Oliver Heirich,
Daniel Gerbeth, Michael Felux, Lukas Marcel Schalk, Dennis Becker,
Nicolas Schneckenburger, Michael Schnell[*]

Abstract

The Ground Based Augmentation System (GBAS) is the cornerstone for enabling automated landings without the Instrument Landing System (ILS). Currently GBAS is evolving to GAST-D for CAT III landings. This extends GBAS via the use of multiple frequencies (L1/L2 and L5) and the use of multiple global navigation satellite system constellations. GBAS requires correction data to be broadcast to aircraft. This is currently done with the VHF Data Broadcast (VDB) datalink. However, VDB has several known shortcomings: (1) low throughput, (2) small area of operation and (3) no cyber-security measures. In this paper we propose the use of the L-band Digital Aeronautical Communications System (LDACS) for broadcasting GBAS correction data to address these shortcomings. In flight experiments conducted in 2019, we set up an experimental GBAS installation using LDACS. Broadcast data was secured using the TESLA broadcast authentication protocol. Our results indicate that cryptographically secured GBAS data via LDACS can provide GAST-C and GAST-D services with high availability if cryptographic parameters are chosen appropriately.

[*]Nils Mäurer, Thomas Gräupl, Miguel A. Bellido-Manganell, Daniel M. Mielke, Alexandra Filip-Dhaubhadel, Oliver Heirich, Daniel Gerbeth, Michael Felux, Lukas Marcel Schalk, Dennis Becker, Michael Schnell are with the Institute of Communications and Navigation of the German Aerospace Center (DLR), Weßling, 82334, Germany. (e-mail: {Nils.Maeurer, Thomas.Graeupl, Miguel.BellidoManganell, Daniel.Mielke, Alexandra.Filip, Oliver.Heirich, Daniel.Gerbeth, Michael.Felux, Lukas.Schalk, Dennis.Becker, Michael.Schnell}@dlr.de). Nicolas Schneckenburger was with the Institute of Communications and Navigation of the German Aerospace Center (DLR) during the preparation and realization of the flight trials (e-mail: nicolas.schneckenburger@gmail.com).

1 Introduction

The Ground Based Augmentation System (GBAS) is used to improve the accuracy of Global Navigation Satellite Systems (GNSSs) to allow GNSS-based instrument landings of aircraft. It is based on reference stations with known positions at the airport, which generate correction data and integrity parameters from GNSS measurements. Correction and integrity data are transmitted to approaching aircraft. Based on these corrections, aircraft can calculate their position with precision and confidence in the integrity of the solution. GBAS enables modern aircraft to perform safe and secure GNSS-based landings while offering several advantages over the Instrument Landing System (ILS) commonly used today: Approaches no longer need to be carried out in a straight line, but can also be curved and with flexible and higher glide angles; it is cheaper than ILS while, at the same time, being transparent in use to the aircrew [1].

GBAS requires a datalink to transmit GNSS correction data to the on-board avionics of the aircraft. As of now, this datalink is specific to GBAS: The VHF Data Broadcast (VDB) datalink.

With GBAS evolving to GBAS Approach Service Type (GAST)-D, which shall enable CAT III landings, VDB becomes a limitation: (1) Current versions of the VDB datalink broadcast only corrections for the L1 frequency of GPS satellites, which is problematic in terms of availability, especially in equatorial zones, due to ionospheric disturbances of the GPS reference measurements required for GBAS [2]. This can be alleviated by extending GBAS with a multi-frequency and multi-constellation approach, including also L5 frequencies and the GALILEO, GLONASS, and BeiDou GNSS systems [3, 4]. However, the VDB datalink is a bottleneck for this extension. It does not provide sufficient throughput for correction and integrity data for multiple constellations and frequencies [5, 6]. Large and complex airports aggravate this issue: In case a single VDB transmitter cannot provide coverage of the complete airport, two transmitters using alternate time slots on the same VDB channel need to be installed, halving datalink capacity. (2) The current VDB service range of 42 km has been criticized as being too small. The criticism is that for pilots to verify that the system is operational an increased range of GBAS services would reduce the pressure and stress level during the final approach. (3) Cyber resilience is also problematic with VDB, since it provides no cyber-security measures comparable to modern wireless systems [7, 8].

These drawbacks show clearly that GBAS would benefit from a more capable datalink supporting its unimpeded evolution. A very good candidate

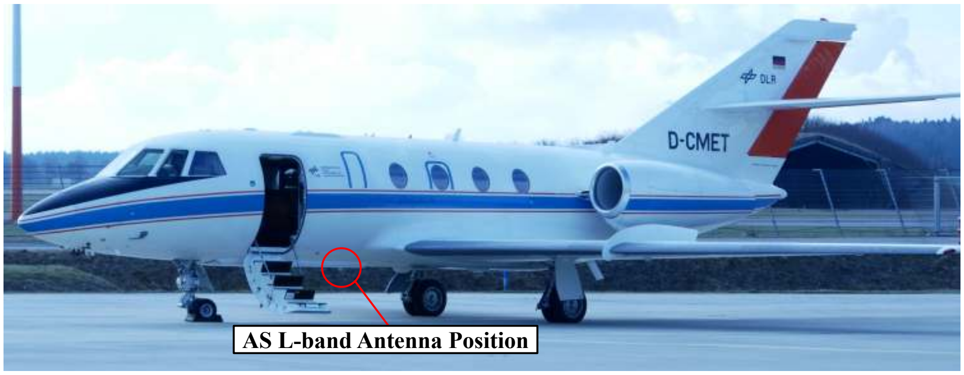


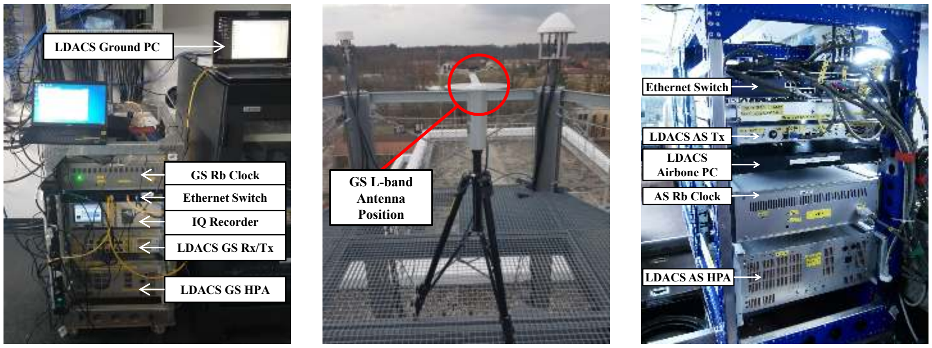
Figure 1: DLR's research aircraft Falcon 20-E5 (D-CMET) used in the experiments.

for a capable GBAS broadcast datalink is the L-band Digital Aeronautical Communications System (LDACS). Currently under ICAO standardization, LDACS is the future aeronautical datalink for applications related to the safety and regularity of flight for terrestrial long-range communications [9].

The objective of this paper is to demonstrate an experimental in-flight implementation of GBAS using L-band Digital Aeronautical Communication System (LDACS) as datalink (1) to multiply the available bandwidth, (2) to increase the service range, and (3) to introduce state-of-the-art broadcast cyber-security using Timed Efficient Stream Loss-tolerant Authentication (TESLA) [10]. The flight trials discussed in this paper were co-funded by the German national research project Migration towards COm/NAV capabilities of LDACS (MICONAV) and took place in March and April 2019. MICONAV also performed other experiments not discussed in this paper.

2 Methodology

The main purpose of the experiments was to demonstrate the ability of LDACS to provide a secure datalink for GBAS. For this purpose we implemented a terrestrial LDACS ground station and GBAS reference station (Figure 2a and 2b), as well as a software-based GBAS receiver. We mounted the receiver on a research aircraft (Figure 1 and 2c) and flew the setup in the vicinity of the ground station.



(a) LDACS ground station (b) LDACS antenna (c) Airborne equipment

Figure 2: Overview of airborne and ground LDACS equipment

2.1 Experimental Setup

The experimental setup consisted of one LDACS aircraft-station and one LDACS ground-station. The GBAS ground-station was co-located with the LDACS ground-station. Figure 3 shows the complete experimental setup in detail: The GBAS ground-station receives GNSS data with a Tallysman TW 3972 antenna, processes it using a JAVAD Sigma unit and passes it to the GBAS ground processing software. The processed GBAS data is passed on to the ground station PC and encrypted with the TESLA protocol before it is transmitted in a message format specific to the experiment. If desired, TESLA encryption can be turned off as indicated in the red box at the center of the diagram. The ground PC is connected to the LDACS ground-station radio via UDP/IP. In the aircraft-station received messages are processed in the reverse order to decrypt GBAS correction data. The correction data is then used by the GBAS software in the aircraft to calculate GBAS Position, Velocity and Time (PVT) and protection levels.

2.1.1 LDACS Datalink Setup

The LDACS aircraft-station was configured for bidirectional communication as specified in [11] and [12]. In addition to LDACS radio equipment, the aircraft-station integrated a Ubuntu 18.04 LTS Linux computer for LDACS and GBAS airborne data processing, and several measurement and storage devices, such as a Rubidium clock, a spectrum analyzer and an I/Q data recorder. Several of these parts are identified in Figure 2c.

The LDACS ground-station, as well as the GBAS ground-station and

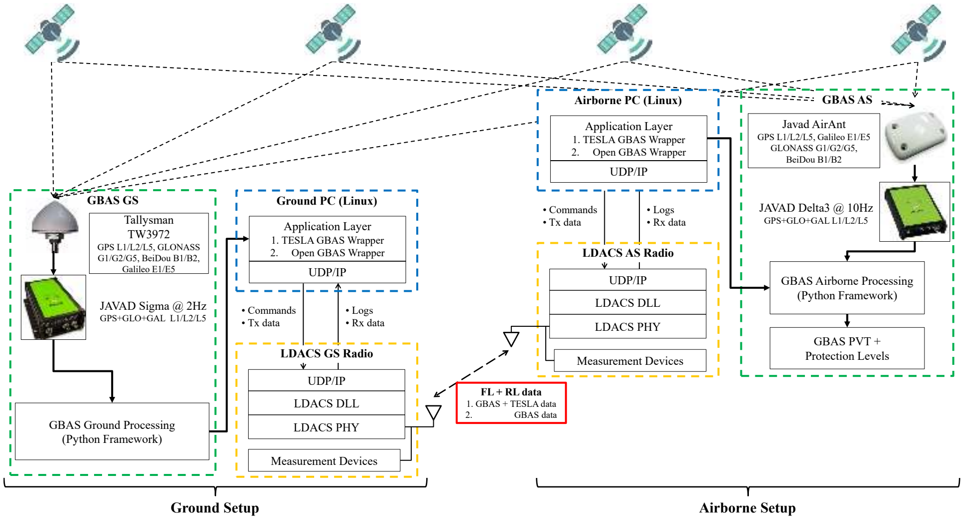


Figure 3: Secure GBAS experimental setup.

antennas were installed on top of an office building at the German Aerospace Center (DLR) premises near Munich, Germany. The LDACS ground-station and its parts are shown in Figure 2a and 2b. The location of the ground-station is indicated in Figure 4.

2.1.2 GBAS Setup

Our experimental setup of the airborne GBAS installation on board the Falcon 20-E5 research aircraft consisted of a Javad air antenna and a Javad Delta 3 unit. This setup was used to receive and process GPS, GLONASS, and Galileo Signals on L1/L2, and L5, and provide data to GBAS airborne processing where the data was combined with the correction data received via LDACS to calculate GBAS PVT and protection levels.

The GBAS ground-station used a Tallysman TW3972 antenna. A Javad Sigma unit was used to process the GPS, GLONASS, and Galileo Signals on L1/L2, and L5 and send the data to GBAS ground processing. This setup is based on the setup discussed in [13]. GBAS air and ground processing was implemented in software in a *python3* application running on Ubuntu 18.04 LTS Linux.

2.1.3 Data Processing

GBAS ground processing generates correction and integrity data from the received GNSS signals. This data is forwarded to the LDACS ground-station software running on the ground station computer. GBAS data can be transmitted to the aircraft in two ways:

1. GBAS data can be encrypted within the TESLA protocol to secure GBAS. The secured GBAS message is then transmitted to the aircraft via LDACS.

2. GBAS data can be left unencrypted. In this case the GBAS message is immediately transmitted to the aircraft via LDACS.

The (1) TESLA secured or (2) unencrypted GBAS data is transmitted from the ground station to the airborne station via LDACS radio messages. The messages received by the LDACS airborne radio are processed and delivered via UDP/IP to the processing Ubuntu 18.04 LTS Linux computer on board the plane. The data is (1) decrypted and authenticated and – if cryptographic authentication succeeded – delivered to the GBAS airborne processing framework. If the GBAS data was not encrypted it is (2) just extracted from the received LDACS messages and immediately forwarded to GBAS airborne processing. GBAS airborne processing combines the received correction and integrity data with the GNSS signals captured by the Javad Air antenna and the Javad Delta-3 receiver to calculate GBAS PVT and protection levels.

2.1.4 TESLA Broadcast Authentication

For the experiment, we implemented a version of the TESLA broadcast authentication protocol to secure GBAS communication over the airgap between ground-station and aircraft-station. TESLA was first proposed by Perrig et al. [10], uses symmetric keys, requires time synchonization between sender and receiver and the ability to buffer messages on the receiver.

Let us assume our communication partners are Alice (the LDACS ground-station) and Bob (the LDACS aircraft-station). For TESLA, we use three functions: a hash function F, to generate a self-authenticated key-chain, a key derivation function F' to derive cryptographic keys for Message Authentication Code (MAC) calculations, another hash function F'' to calculate MACs for a message m. First, Alice splits time in equal intervals T_{int}. Alice then generates a self-authenticated key-chain (e.g. by choosing a random start value and then applying a suitable hash function F iteratively) and assigns each key k_i to its respective interval i of length T_{int}. Then via a key derivation function F' and with key k_i as input, cryptographic keys for MAC calculations is generated for every interval i (e.g. $F'(k_i) = k'_i$). The MACs are calculated on the messages m_i sent out in their respective interval i using function F'' and key k'_i and message m_i as input (e.g. $\mathrm{MAC}_i = F''(k'_i, m_i)$). When Alice sends out messages, Bob can immediately receive them and buffers them until he can verify the MAC. This is not possible for Bob yet, as Alice delays the publication of the key K_i, which is required for the calculation of the MAC of message m_i in interval i, by a certain time interval d. With that, Alice ascertains that at time T_i – the time the message was generated and sent by Alice – only she knew the key for the calculation of the MAC of that message. Releasing the key K_i d intervals later, Bob can verify the correctness of the MAC of previously received and buffered messages. Verification of correctness of MAC_i proofs to Bob (or any other party receiving the broadcast message), that the message m_i with MAC_i was actually sent by Alice, since no one else knew the key k_i at time T_i.

For Bob to partake in the TESLA protocol, Alice and Bob need to synchronize their clocks within a margin of acceptable error [10]. Then Alice sends TESLA parameters such as functions F, F' and F'', the time interval schedule consisting of interval duration T_{int}, start time T_i, index of interval i and the length of the one-way chain, the key disclosure delay d, and a key commitment to the key chain, allowing Bob to verify that the received keys are actually part of the key-chain. These parameters needs to be distributed in an authenticated manner. In the experiment public keys and certificates of the ground-station and aircraft-station were bilaterally exchange via LDACS. In an operational deployment of LDACS the distribution of public keys and certificates will likely be realized via an LDACS specific public key infrastructure, as described in [14, 15, 16, 17]. Knowing Alice's public key, Bob can verify the authenticity of the TESLA parameters and start buffering messages sent by Alice until he receives the correct key to verify their authenticity.

Note, that TESLA authentication requires the buffering of received messages until Alice's authentication key has been received. This introduces a key disclosure delay increasing the communication latency between Alice and Bob.

Time synchronization between aircraft-station and ground-station were implemented as described in [10]. The exchange of TESLA parameters was signed via an Ed25519 digital signature of the ground-station. Our implementation used *python3* and the *nacl* [18] crypto-libary with F being the SHA-512 hash function for key stream generation and two variations F', F''

of the *blake2b* hash function for MAC key derivation and MAC generation.

2.1.5 Limitations of the Experimental Setup

Our experiments used a single GBAS ground receiver with limited ground monitoring, thus without ionosphere and ephemeris monitoring or B-value checks. However this has no influence on the purpose of the experiment, thus it characterizes GBAS over LDACS similar as proposed in [8].

GBAS corrections and integrity parameters were generated and broadcast for GPS, Galileo, and GLONASS for L1 100s and L5 100s processing modes. As we used the LDACS message format, we did not transmit Final Approach Segment (FAS) data and did not use the VDB message format. Transmission of all data was combined in one correction/integrity message per epoch. Producing corrections for all visible satellites our experimental setup generated data rates as predicted in [8]: Approximately 3500 Byte/s, distributed over several communication packets per second. To allow for better characterization of LDACS performance each set of corrections (every 0.5 s) was sent twice with the redundant second message 0.2 s delayed.

The position of the antenna on the aircraft was in an unfavorable place between the wings under the belly of the aircraft. This was due to the availability of port-holes in the experimental aircraft (c.f. Figure 1).

2.2 Flight Trajectories and Experiments

We performed six experiments in two flights. We chose two different flight trajectories to demonstrate secure GBAS via LDACS with different pitch and roll alignments of the aircraft-station and ground-station antennas. During the first flight we transmitted only TESLA secured GBAS via LDACS. We varied the key verification delay to compare different TESLA parameters for GBAS performance. In the second flight the first two experiments were conducted with unsecured GBAS via LDACS, while the last experiment used TESLA again. Flight 2 used a more efficient GBAS message format. The experiments are summarized in Table 1. Both flights included considerable taxiing times and preparation times on the apron not included in the table.

The first flight took place on the 26th of March 2019, had takeoff at 08:53 UTC, touch down at 10:50 UTC, and was chosen as dedicated test flight to demonstrate secure GBAS. Its total airtime was 7000 s with a distance of 1048 km covered. Our goal was to climb, remain at a constant altitude of 6000 m for as long as possible to have different pitch and roll configurations

Experiment	Trajectory	Time (s)	Security	Parameters
01	Flight 1	762.160	TESLA	$T_{int} = 1s\ d = 1$
02	Flight 1	3,755.519	TESLA	$T_{int} = 1s\ d = 2$
03	Flight 1	1,459.296	TESLA	$T_{int} = 1s\ d = 2$
04	Flight 2	1,213.501	unsecured	improved msg. format
05	Flight 2	2,765.582	unsecured	improved msg. format
06	Flight 2	3,028.761	TESLA	$T_{int} = 1s\ d = 2$ improved msg. format

Table 1: Flight trajectories and experiments.

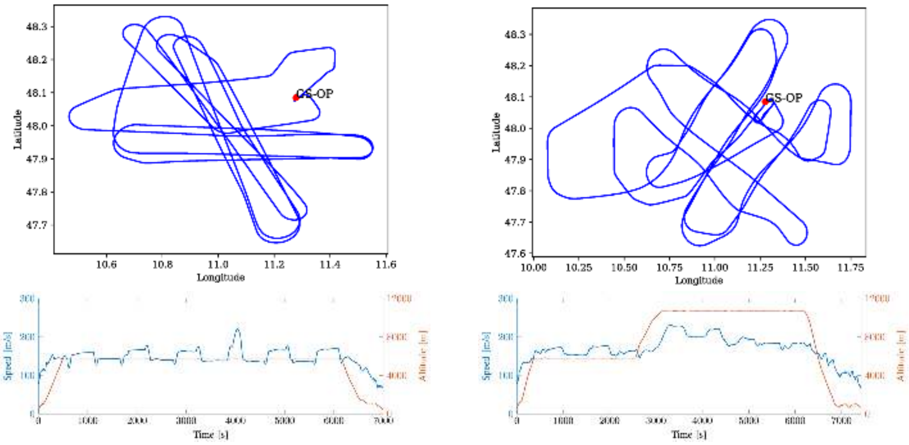
towards the ground-station antenna at constant altitude, and then descend and land, which we achieved as plotted in figure 4a.

The second flight trajectory was used to directly compare TESLA secured GBAS via LDACS and unsecured GBAS via LDACS in several experiments during the same flight. We chose a greater distance to our ground-station, two different flight altitudes, steeper and longer curves and missed approaches provoking and resulting in more antenna shadowing. We achieved all of these prerequisites as shown in figure 4b. Takeoff was on the 2nd of April 2019 at 14:03 UTC, touch down at 16:06 UTC with a total flight time of 7424 s and 1291 km covered with the trajectory depicted in Figure 4b.

3 Results

The quality of GBAS is determined by its availability. We use “GAST-C” and “GAST-D” availability according to RTCA DO-253D [19], sections 2.3.8.1.3.1 and 2.3.11.5.2.1.1/2.

We start with a detailed view around the airport, measuring the GBAS correction age in Fig. 5a. As GBAS is designed as a landing system, but also for ground guidance, taxiing and guided departures are of great interest in the future. Figure 5a shows GBAS correction age during arrival, departure (flight 1), 3 go-arounds (flight 2), and taxiing. Throughout the taxiing and in the air close to the airport we experienced stable performance with correction ages well below the requirements with a single short (10 s) LDACS outage during one of the go-arounds. Note that taxiways and runways are covered although the ground-station antenna is shadowed by a hangar building. Figure 5b shows the availability of the GBAS solutions over the entire course of flight 2. We see that in most situations during flight 2 we had



(a) Flight 1.

(b) Flight 2.

Figure 4: Trajectory, speed and altitude of secure GBAS via LDACS experimental flights. The location of the ground station is marked “GS-OP” for Ground-Station Oberpfaffenhofen near Munich, Germany.

GAST-D coverage implying a GBAS correction age of less than two seconds. Analyzing the median and 95% percentile ($P_{95\%}$) of the correction age in Table 2 these observations are confirmed.

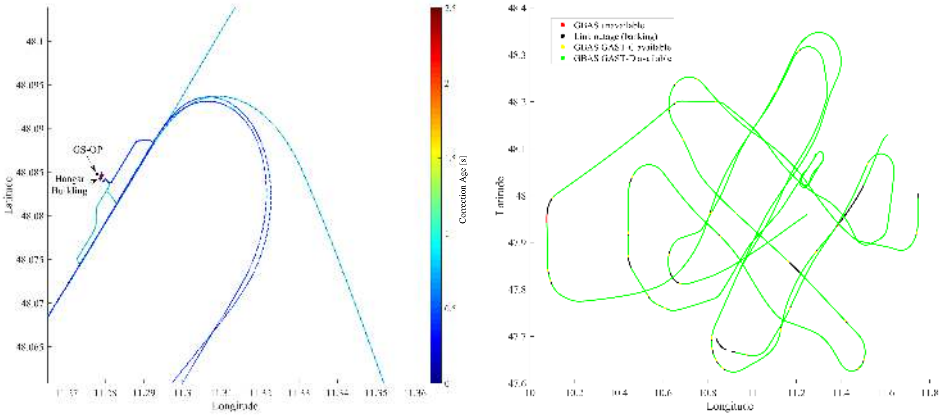
Note, that in experiments 01 - 03 one GBAS message was fragmented into five LDACS packets. In experiments 04 - 06 a more efficient message format was used. No fragmentation was needed in these experiments. This resulted in lower correction ages for flight 2.

3.1 Increased Datalink Throughput

Our experiments generated and transmitted GBAS correction and integrity data for GPS, GLONASS, and Galileo on L1/L2, and L5. The measured offered load and throughput on the LDACS data link is presented in Table 3. Our results indicate that depending on the GBAS update rate 31-50 kbps were required for GBAS GAST-D services in dual-frequency and multi-constellation mode. The difference in data load between flight 1 and 2 is a result of a change of the experimental GBAS message format. Note that the generated GBAS data also depends on the number of visible satellites. Taking into account that the minimum data rate offered by LDACS is 300 kbps in the ground-to-air direction, LDACS offers more than enough capacity

Exp.	Security	Median Cor. Age	$P_{95\%}$ Cor. Age	GAST-C Availability	GAST-D Availability
Flight 1 (GBAS message fragmented in 5 LDACS packets)					
01	after TESLA ($d = 1$)	1.8s	2.2s	88.17%	87.40%
	before authentication	0.9s	1.3s	99.92%	99.84%
02	after TESLA ($d = 2$)	2.8s	3.3s	97.91%	97.90%
	before authentication	0.9s	1.3s	99.40%	99.40%
03	after TESLA ($d = 2$)	2.8s	3.2s	99.30%	99.30%
	before authentication	0.9s	1.3s	99.84%	99.84%
Flight 2 (GBAS message not fragmented)					
04	unsecured	0.4s	0.6s	99.98%	99.98%
05	unsecured	0.4s	0.6s	99.66%	99.61%
06	after TESLA ($d = 2$)	2s	2.6s	97.61%	97.61%
	before authentication	0.4s	0.6s	99.97%	99.97%

Table 2: GBAS via LDACS correction age and availability. Note that experiment 04 and 05 did not employ TESLA. In all other experiments GBAS availability has been measured before and after TESLA authentication.



(a) GBAS correction age at EDMO Airport.

(b) GBAS availability in flight 2.

Figure 5: Age of GBAS correction data in the experiments.

Exp.	Duration in (s)	Avg. Offered Load in (kbps)	Avg. Throughput in (kbps)	Loss in %
Flight 1				
01	762.160	49.80	49.31	0.99
02	3,755.519	45.56	44.94	1.37
03	1,459.296	48.10	47.93	0.36
Flight 2				
04	1,213.501	34.58	34.43	0.43
05	2,765.582	34.19	33.86	0.94
06	3,028.761	31.69	31.37	1.01

Table 3: GBAS over LDACS datalink throughput.

to support GBAS, Air Traffic Services (ATS) or Aeronautical Operational Control (AOC) on the same channel.

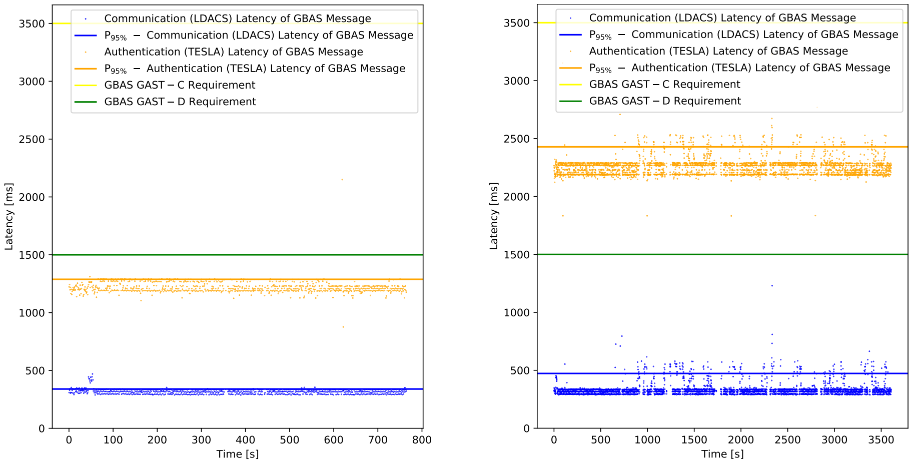
3.2 Increased Service Range

The LDACS specification [20] stipulates at a maximum averaged EIRP of 52 dBm resulting in maximum designed communication range of 200 NM. However, local regulations allowed us to transmit only an EIRP of 40 dBm in our experiments. This reduction of 12 dBm – assuming free-space path loss – should result in a reduced communication range of at least 50 NM (92.6 km).

During the testing of GBAS in flights 1 and 2 we reached a maximum distance of 61 km and 94 km respectively. On both occasions we could send and receive GBAS packets, making the maximum demonstrated GBAS via LDACS service range in in our experiment 94 km. As the service volume of GBAS contains 42 km around the local ground facility with the VDB datalink, we demonstrated the possibility to double that distance with 12 dBm EIRP less than foreseen for an operational LDACS deployment.

3.3 Cyber-Security

TESLA security adds a configurable key disclosure delay to the authentication latency. We chose conservative key disclosure delays for our experiments and set the interval length to one second ($T_{int} = 1s$) and the key delay to one time interval ($d = 1$) for experiment 01 and two intervals ($d = 2$) for all other experiments.



(a) Experiment 01 ($T_{int} = 1s$, $d = 1$) (b) Experiment 02 ($T_{int} = 1s$, $d = 2$)

Figure 6: Latencies of secured GBAS messages. Note that the GBAS messages in experiment 01 and 02 have been fragmented into five LDACS packets. Latency can be improved with the more efficient message format used in flight 2.

Changing the key delay resulted in different authentication latency measurements. Secure GBAS messages sent in experiment 01 experienced approximately one second less latency. This verifies the correctness of the implementation of the TESLA protocol, as in experiment 01 all messages can already be verified when they have received the key in the next message ($d = 1$), whereas in all other experiments, the right key is contained in the message after the next message ($d = 2$). The one second difference in authentication latency is clearly visible in Figure 6a and 6b. Note that the latency values of these figures are not directly comparable to the correction ages presented in Table 2. The GBAS correction age is measured relative to the start of the GBAS epoch, the communication latency is not.

TESLA cyber-security adds additional load to the datalink. TESLA added on average 104 B per secured GBAS message. Time synchronization and parameter exchange during the set up of TESLA added additional 2145 B to each experiment. This resulted in an average security data overhead of 7.43% per message.

4 Discussion

Safety and security are strongly interrelated in aviation which makes strong cyber-security a key enabler for digitalization in aviation [21]. Unfortunately cyber-security for aeronautical communication is still not realized in most deployed systems [22, 23]. Terrestrial datalinks such as VDB have a low data rate of 28.416 kbps and no state-of-the-art cyber-security features [24, 21, 23].

In our experiments we demonstrated a viable alternative to VDB offering at least 10 times the net capacity in data rate and profound cyber-security measures. With TESLA on top of LDACS, we have shown that additional dedicated broadcast message authentication is realistic and feasible. An important result is that all TESLA authenticated messages, that reached the aircraft, could be verified. This showed the good choice of TESLA as broadcast authentication protocol, as all GBAS messages secured via TESLA could be verified to have been sent by an authentic ground station. This, and our analysis of throughput and latency show that TESLA provides good security for GBAS via LDACS with reasonable security overhead and acceptable latency.

The latency of LDACS is sufficient to enable time shifted broadcast authentication protocol such as TESLA. However, we have seen that the parameter choice of TESLA is important here. Up to a delay of one second, the latency for TESLA secured GBAS messages via LDACS remains low enough to stay within the requirements for GAST-C and GAST-D services. Tweaking the time interval and key delay times might lead to even shorter latencies than demonstrated in our experiments.

LDACS offers at least a range of 94 km for GBAS service. With higher LDACS transmission power this range could be drastically increased to 200 NM. However, depending on the region and the local properties of the ionosphere, GBAS correction data may not necessarily be useful more than 100 NM away from the reference station [25, 26]. However, the current GBAS service volume of 42 km was criticized as too small in the past. The argument is that the corrections are not used beyond the service volume point for landing service but from the intercept point to the final approach, but for the pilot to verify that the system is already operational. An increased range of GBAS services would reduce the pressure and stress level of the pilots during the final approach, as they can check availability and operational correctness of the GBAS service significantly earlier than today.

GBAS has only a minor siting problem concerning VDB, however, LDACS may offer improvements here, too. Siting problems are often related to the reference antennas, VDB is not so critical and often simply co-located with the VHF communication antennas. There are, however, large complex airports like Frankfurt where a VDB transmitter cannot ensure coverage on all runways. Today those airports work with two VDB transmitters on the same channel which halves the capacity due to alternating slots. A different technical solution not halving the capacity of the data link is very much desirable. This solution must ensure coverage on all runways for the rollout guidance up to 12 ft above the ground. With our demonstration of GBAS via LDACS on the apron, taxiway, and runway, we demonstrated that LDACS can provide such a solution.

5 Conclusion

Our experiments demonstrated, that multi-constellation, multi-frequency GBAS can be realized using LDACS efficiently and securely.

Also, LDACS may provide additional benefits to GBAS: It offers enough data-rate to broadcast cryptographically secured GBAS data, while offering spare capacity for other Air Traffic Services (ATS) or Aeronautical Operational Control (AOC) services on the same channel. We have shown that LDACS can extend the GBAS service range into the order of 100 km. And we have seen, that GBAS via LDACS works in non-line-of-sight situations with approximately the same GBAS availability as measured during flight. We demonstrated the possibility to protect broadcast data with the broadcast authentication protocol TESLA. Our results show, that TESLA is well suited for securing GBAS data via LDACS, however TESLA parameters have to be chosen carefully.

The advantages of GBAS over LDACS – (1) increased data rate, (2) increased range, and (3) cyber-security – indicate clearly that further development of secure GBAS over LDACS may be a key enabler for the future evolution of GBAS.

6 Acronyms

DLR	German Aerospace Center
FAS	Final Approach Segment
GAST	GBAS Approach Service Type
GBAS	Ground Based Augmentation System
GNSS	Global Navigation Satellite System

ILS	Instrument Landing System
LDACS	L-band Digital Aeronautical Communication System
MAC	Message Authentication Code
MICONAV	Migration towards COm/NAV capabilities of LDACS
PVT	Position, Velocity and Time
TESLA	Timed Efficient Stream Loss-tolerant Authentication
VDB	VHF Data Broadcast

References

[1] M. Felux, T. Dautermann, and H. Becker, "GBAS landing system–precision approach guidance after ILS," *Aircraft Engineering and Aerospace Technology*, 2013.

[2] J. Lee and M. Kim, "Optimized GNSS station selection to support long-term monitoring of ionospheric anomalies for aircraft landing systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 1, pp. 236–246, 2017.

[3] M.-S. Circiu, M. Felux, B. Belabbas, M. Meurer, J. Lee, M. Kim, and S. Pullen, "Evaluation of GPS L5, Galileo E1 and Galileo E5a performance in flight trials for multi frequency multi constellation GBAS," *Proceedings of ION GNSS+ 2015*, 2015.

[4] D. Gerbeth, M. Felux, M.-S. Circiu, and M. Caamano, "Optimized selection of satellite subsets for a multi-constellation GBAS," *Proc. ION Int'l. Tech. Mtg., Monterey CA*, 2016.

[5] T. Feuerle, M. Stanisak, S. Saito, T. Yoshihara, and A. Lipp, "GBAS interoperability trials and multi-constellation/multi-frequency ground mockup evaluation," *Proceedings of the 6th SESAR innovation days*, 2016.

[6] M. Stanisak, A. Lipp, and T. Feuerle, "Possible VDB formatting for multi-constellation/multi-frequency GBAS services," in *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS'15)*, pp. 1507–1518, 2015.

[7] J. García, "Broadband connected aircraft security," in *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, pp. 1–23, IEEE, 2015.

[8] M. Felux, T. Gräupl, N. Mäurer, and M. Stanisak, "Transmitting GBAS messages via LDACS," in *37th Digital Avionics Systems Conference (DASC)*, (New York, NY, USA), pp. 1–7, IEEE, September 2018.

[9] M. Schnell, "Update on LDACS - The FCI Terrestrial Data Link," in *19th Integrated Communications, Navigation and Surveillance Conference (ICNS)*, (New York, NY, USA), pp. 1–10, IEEE, April 2019.

[10] A. Perrig and J. Tygar, "TESLA Broadcast Authentication," *Secure Broadcast Communication*, pp. 29–53, 2003.

[11] M. Sajatovic, B. Haindl, U. Epple, and T. Gräupl, "Updated LDACS1 System Specification," SESAR2020 PJ14-02-01 D3.3.010 00.01.01, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, 2017 (accessed July 9, 2019).

[12] International Civil Aviation Organization (ICAO), "Finalization of LDACS Draft SARPs," tech. rep., ICAO, Montreal, CA, Oct 2018.

[13] M.-S. Circiu, M. Felux, D. Gerbeth, M. Caamano, and M. Meurer, "Assessment of Different Dual-frequency Dual-constellation GBAS Processing Modes based on Flight Trials," *Proceedings of ION GNSS+ 2016*, September 2016.

[14] Mäurer, N. and Bilzhause, A., "A cyber-security Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *37th Digital Avionics Systems Conference (DASC)*, (New York, NY, USA), pp. 1–10, IEEE, September 2018.

[15] N. Mäurer and C. Schmitt, "Towards Successful Realization of the LDACS cyber-security Architecture: An Updated Datalink Security Threat- and Risk Analysis," in *19th Integrated Communications, Navigation and Surveillance Conference (ICNS)*, (New York, NY, USA), pp. 1A2/1–1A2–13, IEEE, April 2019.

[16] N. Mäurer, T. Gräupl, and C. Schmitt, "Evaluation of the ldacs cybersecurity implementation," in *38th Digital Avionics Systems Conference (DASC)*, pp. 1–10, IEEE, September 2019.

[17] Mäurer, N., Gräupl, T. and Schmitt, C., "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *39th Digital Avionics Systems Conference (DASC)*, (New York, NY, USA), pp. 1–10, IEEE, October 2020.

[18] D. J. Bernstein, "Cryptography in NaCl," *Networking and Cryptography library*, vol. 3, p. 385, 2009.

[19] Radio Technical Commission for Aeronautics (RTCA), "Minimum Operational Performance Standards for GPS Local Area Augmentation System," tech. rep., RTCA, Washington, DC, US, July 2017.

[20] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," sesar2020 pj14-02-01 d3.3.030, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, 2019.

[21] M. Slim, B. Mahmoud, A. Pirovano, and N. Larrieu, "Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey," *Computer Science Review*, vol. 11-12, pp. 1–29, May 2014.

[22] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *Black Hat USA*, August 2012.

[23] M. Niraula, J. Graefe, R. Dlouhy, M. Layton, and M. Stevenson, "ATN/IPS security approach: Two-way mutual authentication, data integrity and privacy," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, pp. 1A3–1, IEEE, 2018.

[24] O. Osechas, M. Mostafa, T. Graupl, and M. Meurer, "Addressing vulnerabilities of the CNS infrastructure to targeted radio interference," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 34–42, 2017.

[25] S. Pullen and P. Enge, "An overview of GBAS integrity monitoring with a focus on ionospheric spatial anomalies," *94.20. Vv; 94.20 B6*, 2007.

[26] S. Saito, S. Sunda, J. Lee, S. Pullen, S. Supriadi, T. Yoshihara, M. Terkildsen, and F. Lecat, "Ionospheric delay gradient model for GBAS in the Asia-Pacific region," *GPS Solutions*, vol. 21, no. 4, pp. 1937–1947, 2017.