RAW
Internet-Draft
Intended status: Informational
Expires: 5 April 2021

N. Maeurer, Ed.
T. Graeupl, Ed.
German Aerospace Center (DLR)
C. Schmitt, Ed.
Research Institute CODE, UniBwM

2 October 2020

L-band Digital Aeronautical Communications System (LDACS)
draft-maeurer-raw-ldacs-06

Abstract

This document provides an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation. LDACS is a scheduled, reliable multi-application cellular broadband system with support for IPv6. LDACS shall provide a data link for IP network-based aircraft guidance. High reliability and availability for IP connectivity over LDACS are therefore essential.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 April 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

One of the main pillars of the modern Air Traffic Management (ATM) system is the existence of a communication infrastructure that enables efficient aircraft control and safe separation in all phases of flight. Current systems are technically mature but suffering from the VHF band's increasing saturation in high-density areas and the limitations posed by analogue radio communications. Therefore, aviation globally and the European Union (EU) in particular, strives for a sustainable modernization of the aeronautical communication infrastructure.

In the long-term, ATM communication shall transition from analogue VHF voice and VDLM2 communication to more spectrum efficient digital data communication. The European ATM Master Plan foresees this transition to be realized for terrestrial communications by the development (and potential implementation) of the L-band Digital Aeronautical Communications System (LDACS). LDACS shall enable IPv6 based air- ground communication related to the aviation safety and regularity of flight. The particular challenge is that no additional spectrum can be made available for terrestrial aeronautical communication. It was thus necessary to develop co-existence mechanism/procedures to enable the interference free operation of

LDACS in parallel with other aeronautical services/systems in the same frequency band.

Since LDACS shall be used for aircraft guidance, high reliability and availability for IP connectivity over LDACS are essential.

2. Terminology

The following terms are used in the context of RAW in this document:

A2A Air-to-Air
LDACS A2A LDACS Air-to-Air

AeroMACS Aeronautical Mobile Airport Communication System
A2G Air-to-Ground
ACARS Aircraft Communications Addressing and Reporting System
ADS-C Automatic Dependent Surveillance - Contract
AM(R)S Aeronautical Mobile (Route) Service
ANSP Air traffic Network Service Provider
AOC Aeronautical Operational Control
AS Aircraft Station
ATC Air-Traffic Control
ATM Air-Traffic Management
ATN Aeronautical Telecommunication Network
ATS Air Traffic Service
CCCH Common Control Channel
COTS IP Commercial Off-The-Shelf
CM Context Management
CNS Communication Navigation Surveillance
CPDLC Controller Pilot Data Link Communication
DCCH Dedicated Control Channel
DCH Data Channel
DLL Data Link Layer
DLS Data Link Service
DME Distance Measuring Equipment
DSB-AM Double Side-Band Amplitude Modulation
FAA Federal Aviation Administration
FCI Future Communication Infrastructure
FDD Frequency Division Duplex
FL Forward Link
GANP Global Air Navigation Plan
GNSS Global Navigation Satellite System

GS	Ground Station
GSC	Ground-Station Controller
G2A	Ground-to-Air
HF	High Frequency
ICAO	International Civil Aviation Organization
IP	Internet Protocol
kbit/s	kilobit per second
LDACS	L-band Digital Aeronautical Communications System
LLC	Logical Link Layer
LME	LDACS Management Entity
MAC	Medium Access Layer
MF	Multi Frame
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiplexing Access
OSI	Open Systems Interconnection
PDU	Protocol Data Units
PHY	Physical Layer
QoS	Quality of Service
RL	Reverse Link
SARPs	Standards And Recommended Practices
SDR	Software Defined Radio
SESAR	Single European Sky ATM Research
SF	Super-Frame
SNP	Sub-Network Protocol
SSB-AM	Single Side-Band Amplitude Modulation
TBO	Trajectory-Based Operations
TDM	Time Division Multiplexing
TDMA	Time-Division Multiplexing-Access
VDLM1	VHF Data Link mode 1
VDLM2	VHF Data Link mode 2
VHF	Very High Frequency
VI	Voice Interface

3. Motivation and Use Cases

Aircraft are currently connected to Air-Traffic Control (ATC) and Aeronautical Operational Control (AOC) via voice and data communications systems through all phases of a flight. Within the airport terminal, connectivity is focused on high bandwidth communications, while during en-route high reliability, robustness, and range is the main focus. Voice communications may use the same or different equipment as data communications systems. In the following the main differences between voice and data communications capabilities are summarized. The assumed use cases for LDACS completes the list of use cases stated in [RAW-USE-CASES] and the list of reliable and available wireless technologies presented in [RAW-TECHNOS].

3.1. Voice Communications Today

Voice links are used for Air-to-Ground (A2G) and Air-to-Air (A2A) communications. The communication equipment is either ground-based working in the High Frequency (HF) or Very High Frequency (VHF) frequency band or satellite-based. All VHF and HF voice communications is operated via open broadcast channels without authentication, encryption or other protective measures. The use of well-proven communication procedures via broadcast channels helps to enhance the safety of communications by taking into account that other users may encounter communication problems and may be supported, if required. The main voice communications media is still the analogue VHF Double Side-Band Amplitude Modulation (DSB-AM) communications technique, supplemented by HF Single Side-Band Amplitude Modulation (SSB-AM) and satellite communications for remote and oceanic areas. DSB-AM has been in use since 1948, works reliably and safely, and uses low-cost communication equipment. These are the main reasons why VHF DSB-AM communications is still in use, and it is likely that this technology will remain in service for many more years. This however results in current operational limitations and impediments in deploying new Air-Traffic Management (ATM) applications, such as flight-centric operation with Point-to-Point communications.

3.2. Data Communications Today

Like for voice, data communications into the cockpit is currently provided by ground-based equipment operating either on HF or VHF radio bands or by legacy satellite systems. All these communication systems are using narrowband radio channels with a data throughput capacity in order of kilobits per second. While the aircraft is on ground some additional communications systems are available, like Aeronautical Mobile Airport Communication System (AeroMACS; as of now not widely used) or public cellular networks, operating in the Airport (APT) domain and able to deliver broadband communication capability.

The data communication networks used for the transmission of data relating to the safety and regularity of the flight must be strictly isolated from those providing entertainment services to passengers. This leads to a situation that the flight crews are supported by narrowband services during flight while passengers have access to inflight broadband services. The current HF and VHF data links cannot provide broadband services now or in the future, due to the lack of available spectrum. This technical shortcoming is becoming a limitation to enhanced ATM operations, such as Trajectory-Based Operations (TBO) and 4D trajectory negotiations.

Satellite-based communications are currently under investigation and enhanced capabilities are under development which will be able to provide inflight broadband services and communications supporting the safety and regularity of flight. In parallel, the ground-based broadband data link technology LDACS is being standardized by ICAO and has recently shown its maturity during flight tests [SCH20191]. The LDACS technology is scalable, secure and spectrum efficient and provides significant advantages to the users and service providers. It is expected that both - satellite systems and LDACS - will be deployed to support the future aeronautical communication needs as envisaged by the ICAO Global Air Navigation Plan (GANP).

4. Provenance and Documents

The development of LDACS has already made substantial progress in the Single European Sky ATM Research (SESAR) framework, and is currently being continued in the follow-up program, SESAR2020 [RIH2018]. A key objective of the SESAR activities is to develop, implement and validate a modern aeronautical data link able to evolve with aviation needs over long-term. To this end, an LDACS specification has been produced [GRA2019] and is continuously updated; transmitter demonstrators were developed to test the spectrum compatibility of LDACS with legacy systems operating in the L-band [SAJ2014]; and the overall system performance was analyzed by computer simulations, indicating that LDACS can fulfil the identified requirements [GRA2011].

LDACS standardization within the framework of the ICAO started in December 2016. The ICAO standardization group has produced an initial Standards and Recommended Practices (SARPs) document [ICA2018]. The SARPs document defines the general characteristics of LDACS. The ICAO standardization group plans to produce an ICAO technical manual - the ICAO equivalent to a technical standard - within the next years. Generally, the group is open to input from all sources and develops LDACS in the open.

Up to now LDACS standardization has been focused on the development of the physical layer and the data link layer, only recently have higher layers come into the focus of the LDACS development activities. There is currently no "IPv6 over LDACS" specification publicly available; however, SESAR2020 has started the testing of IPv6-based LDACS testbeds.

The IPv6 architecture for the aeronautical telecommunication network is called the Future Communications Infrastructure (FCI). FCI shall support quality of service, diversity, and mobility under the umbrella of the "multi-link concept". This work is conducted by ICAO Communication Panel working group WG-I.

In addition to standardization activities several industrial LDACS prototypes have been built. One set of LDACS prototypes has been evaluated in flight trials confirming the theoretical results predicting the system performance [GRA2018] [SCH20191].

5. Applicability

LDACS is a multi-application cellular broadband system capable of simultaneously providing various kinds of Air Traffic Services (including ATS-B3) and Aeronautical Operational Control (AOC) communications services from deployed Ground Stations (GS). The LDACS A2G sub-system physical layer and data link layer are optimized for data link communications, but the system also supports digital air-ground voice communications.

LDACS supports communication in all airspaces (airport, terminal maneuvering area, and en-route), and on the airport surface. The physical LDACS cell coverage is effectively de-coupled from the operational coverage required for a particular service. This is new in aeronautical communications. Services requiring wide-area coverage can be installed at several adjacent LDACS cells. The handover between the involved LDACS cells is seamless, automatic, and transparent to the user. Therefore, the LDACS A2G communications concept enables the aeronautical communication infrastructure to support future dynamic airspace management concepts.

5.1. Advances Beyond the State-of-the-Art

LDACS offers several capabilities that are not provided in contemporarily deployed aeronautical communication systems.

5.1.1. Priorities

LDACS is able to manage services priorities, an important feature not available in some of the current data link deployments. Thus, LDACS guarantees bandwidth, low latency, and high continuity of service for safety critical ATS applications while simultaneously accommodating less safety-critical AOC services.

5.1.2. Security

LDACS is a secure data link with built-in security mechanisms. It enables secure data communications for ATS and AOC services, including secured private communications for aircraft operators and ANSPs (Air Navigation Service Providers). This includes concepts for key and trust management, mutual authenticated key exchange protocols, key derivation measures, user and control message-in-transit confidentiality and authenticity protection, secure logging and availability and robustness measures [MAE20181], [MAE20191], [MAE20192].

5.1.3. High Data Rates

The user data rate of LDACS is 315 kbit/s to 1428 kbit/s on the forward link (Ground-to-Air), and 294 kbit/s to 1390 kbit/s on the reverse link (Air-to-Ground), depending on coding and modulation. This is 50 times the amount terrestrial digital aeronautical communications systems such as VDLM2 provide [SCH20191].

5.2. Application

LDACS shall be used by several aeronautical applications ranging from enhanced communication protocol stacks (multi-homed mobile IPv6 networks in the aircraft and potentially ad-hoc networks between aircraft) to classical communication applications (sending GBAS correction data) and integration with other service domains (using the communication signal for navigation).

5.2.1. Air-to-Ground Multilink

It is expected that LDACS together with upgraded satellite-based communications systems will be deployed within the Future Communication Infrastructure (FCI) and constitute one of the main components of the multilink concept within the FCI.

Both technologies, LDACS and satellite systems, have their specific benefits and technical capabilities which complement each other. Especially, satellite systems are well-suited for large coverage areas with less dense air traffic, e.g. oceanic regions. LDACS is well-suited for dense air traffic areas, e.g. continental areas or hot-spots around airports and terminal airspace. In addition, both technologies offer comparable data link capacity and, thus, are well-suited for redundancy, mutual back-up, or load balancing.

Technically the FCI multilink concept shall be realized by multi-homed mobile IPv6 networks in the aircraft. The related protocol stack is currently under development by ICAO and SESAR.

5.2.2. Air-to-Air Extension for LDACS

A potential extension of the multi-link concept is its extension to ad-hoc networks between aircraft.

Direct Air-to-Air (A2A) communication between aircrafts in terms of ad-hoc data networks is currently considered a research topic since there is no immediate operational need for it, although several possible use cases are discussed (digital voice, wake vortex warnings, and trajectory negotiation) [BEL2019]. It should also be noted that currently deployed analog VHF voice radios support direct voice communication between aircraft, making a similar use case for digital voice plausible.

LDACS direct A2A is currently not part of standardization.

5.2.3. Flight Guidance

The FCI (and therefore LDACS) shall be used to host flight guidance. This is realized using three applications:

1. Context Management (CM): The CM application shall manage the automatic logical connection to the ATC center currently responsible to guide the aircraft. Currently this is done by the air crew manually changing VHF voice frequencies according to the progress of the flight. The CM application automatically sets up equivalent sessions.
2. Controller Pilot Data Link Communication (CPDLC): The CPDLC application provides the air crew with the ability to exchange data messages similar to text messages with the currently responsible ATC center. The CPDLC application shall take over most of the communication currently performed over VHF voice and enable new services that do not lend themselves to voice communication (e.g., trajectory negotiation).
3. Automatic Dependent Surveillance - Contract (ADS-C): ADS-C reports the position of the aircraft to the currently active ATC center. Reporting is bound to "contracts", i.e. pre-defined events related to the progress of the flight (i.e. the trajectory). ADS-C and CPDLC are the primary applications used to implement in-flight trajectory management.

CM, CPDLC, and ADS-C are available on legacy datalinks, but not widely deployed and with limited functionality.

Further ATC applications may be ported to use the FCI or LDACS as well. A notable application is GBAS for secure, automated landings: The Global Navigation Satellite System (GNSS) based Ground Based Augmentation System (GBAS) is used to improve the accuracy of GNSS to allow GNSS based instrument landings. This is realized by sending GNSS correction data (e.g., compensating ionospheric errors in the GNSS signal) to the airborne GNSS receiver via a separate data link. Currently the VDB data link is used. VDB is a narrow-band single-purpose datalink without advanced security only used to transmit GBAS correction data. This makes VDB a natural candidate for replacement by LDACS.

5.2.4. Business Communication of Airlines

In addition to air traffic services AOC services shall be transmitted over LDACS. AOC is a generic term referring to the business communication of airlines. Regulatory this is considered related to the safety and regularity of flight and may therefore be transmitted over LDACS.

AOC communication is considered the main business case for LDACS communication service providers since modern aircraft generate significant amounts of data (e.g., engine maintenance data).

5.2.5. LDACS Navigation

Beyond communication radio signals can always also be used for navigation. LDACS takes this into account.

For future aeronautical navigation, ICAO recommends the further development of Global Navigation Satellite System (GNSS) based technologies as primary means for navigation. However, the drawback of GNSS is its inherent single point of failure - the satellite. Due to the large separation between navigational satellites and aircraft, the received power of GNSS signals on the ground is very low. As a result, GNSS disruptions might occasionally occur due to unintentional interference, or intentional jamming. Yet the navigation services must be available with sufficient performance for all phases of flight. Therefore, during GNSS outages, or blockages, an alternative solution is needed. This is commonly referred to as Alternative Positioning, Navigation, and Timing (APNT).

One of such APNT solution consists of integrating the navigation functionality into LDACS. The ground infrastructure for APNT is deployed through the implementation of LDACS ground stations and the navigation capability comes "for free".

LDACS navigation has already been demonstrated in practice in a flight measurement campaign [SCH20191].

6. Requirements to LDACS

The requirements to LDACS are mostly defined by its application area: Communication related to safety and regularity of flight.

A particularity of the current aeronautical communication landscape is that it is heavily regulated. Aeronautical data links (for applications related to safety and regularity of flight) may only use spectrum licensed to aviation and data links endorsed by ICAO. Nation states can change this locally, however, due to the global scale of the air transportation system adherence to these practices is to be expected.

Aeronautical data links for the Aeronautical Telecommunication Network (ATN) are therefore expected to remain in service for decades. The VDLM2 data link currently used for digital terrestrial internetworking was developed in the 1990es (the use of the OSI internetwork stack indicates that as well). VDLM2 is expected to be used at least for several decades. In this respect aeronautical communication (for applications related to safety and regularity of flight) is more comparable to industrial applications than to the open Internet.

Internetwork technology is already installed in current aircraft. Current ATS applications use either the Aircraft Communications Addressing and Reporting System (ACARS) or the Open Systems Interconnection (OSI) stack. The objective of the development effort LDACS is part of (FCI) is to replace legacy (OSI) and proprietary (ACARS) internetwork technologies with industry standard IP technology. It is anticipated that the use of Commercial Off-The-Shelf (COTS) IP technology mostly applies to the ground network. The avionics networks on the aircraft will likely be heavily modified or proprietary.

AOC applications currently mostly use the same stack (although some applications, like the graphical weather service may use the commercial passenger network). This creates capacity problems (resulting in excessive amounts of timeouts) since the underlying terrestrial data links (VDLM1/2) do not provide sufficient bandwidth. The use of non-aviation specific data links is considered a security problem. Ideally the aeronautical IP internetwork and the Internet should be completely separated.

The objective of LDACS is to provide a next generation terrestrial data link designed to support IP and provide much higher bandwidth to avoid the currently experienced operational problems.

The requirement for LDACS is therefore to provide a terrestrial high-throughput data link for IP internetworking in the aircraft.

In order to fulfil the above requirement LDACS needs to be interoperable with IP (and IP-based services e.g. VoIP) at the gateway connecting the LDACS network to other aeronautical ground networks (the totality of them being the ATN). On the avionics side in the aircraft aviation specific solutions are to be expected.

In addition to the functional requirements LDACS and its IP stack need to fulfil the requirements defined in RTCA DO-350A/EUROCAE ED-228A [DO350A]. This document defines continuity, availability, and integrity requirements at different scopes for each air traffic management application (CPDLC, CM, and ADS-C). The scope most relevant to IP over LDACS is the CSP (Communication Service Provider) scope.

The upcoming Figures Figure 1 and Figure 2 summarize the main seetings based on volume 1 Table 5-14, and Table 6-13 defined in [DO350A]. In a similar vein, requirements to fault management are defined in the same tables.

	ECP 130		RCP 240		RCP 400	
Parameter	ET	TT_95%	ET	TT_95%	ET	TT_95%
Transaction Time (Sec)	130	67	240	210	400	350
Continuity	0.999	0.95	0.999	0.95	0.999	0.95
Availability	0.989		0.989 (safety)		0.989	

		0.9899 (efficiency)	
Integrity	1E-5 per FH	1E-5 per FH	1E-5 per FH
RCP Monitoring and Alerting Criteria			
MA-1	The system shall be capable of detecting failures and configuration changes that would cause the communication service no longer meet the RCP specification for the intended use.		
MA-2	When the communication service can no longer meet the RCP specification for the intended function, the flight crew and/or the controller shall take appropriate action.		

Figure 1: Requirements for CPDLC

	RSP 160		RSP 180		RSP 400	
Parameter	OT	DT 95%	OT	DT 95%	OT	DT 95%

Transaction time (sec)	160	90	180	90	400	300
Continuity	0.999	0.95	0.999	0.95	0.999	0.95
Availability	0.989		0.989 (safety) 0.9899 (efficiency)		0.989	
Integrity	1E-5 per FH		1E-5 per FH		1E-5 per FH	
RCP Monitoring and Alerting Criteria						
MA-1	The system shall be capable of detecting failures and configuration changes that would cause the ADS-C service no longer meet the RSP specification for the intended function.					
MA-2	When the ADS-C service can no longer meet the RSP specification for the intended function, the flight crew and/or the controller shall take appropriate action.					

Figure 2: Requirements for ADS-C

7. Characteristics of LDACS

LDACS will become one of several wireless access networks connecting aircraft to the ATN implemented by the FCI and possibly ACARS/FANS networks [FAN2019].

The current LDACS design is focused on the specification of layer 2.

Achieving stringent the continuity, availability, and integrity requirements defined in [DO350A] will require the specification of layer 3 and above mechanisms (e.g. reliable crossover at the IP layer). Fault management mechanisms are similarly undefined. Input from the working group will be appreciated here.

7.1. LDACS Sub-Network

An LDACS sub-network contains an Access Router (AR), a Ground-Station Controller (GSC), and several Ground-Stations (GS), each of them providing one LDACS radio cell.

User plane interconnection to the ATN is facilitated by the Access Router (AR) peering with an Air-to-Ground Router (A2G Router) connected to the ATN. It is up to implementer's choice to keep Access Router and Air-Ground Router functions separated, or to merge them.

The internal control plane of an LDACS sub-network is managed by the GSC. An LDACS sub-network is illustrated in Figure 3.

```
   wireless      user
   link          plane
     A--------------G-------------Access---A2G-----ATN
     S..............S             Router   Router
                    . control      . |
                    . plane        . |
                    .              . |
                    GSC..............|
                    .                |
                    .                |
                    GS---------------+
```

Figure 3: LDACS sub-network with two GSs and one AS

7.2. Topology

LDACS operating in A2G mode is a cellular point-to-multipoint system. The A2G mode assumes a star-topology in each cell where Aircraft Stations (AS) belonging to aircraft within a certain volume of space (the LDACS cell) is connected to the controlling GS. The LDACS GS is a centralized instance that controls LDACS A2G communications within its cell. The LDACS GS can simultaneously support multiple bi-directional communications to the ASs under its control. LDACS ground stations themselves are connected to a GSC controlling the LDACS sub-network.

Prior to utilizing the system an AS has to register with the controlling GS to establish dedicated logical channels for user and control data. Control channels have statically allocated resources, while user channels have dynamically assigned resources according to the current demand. Logical channels exist only between the GS and the AS.

The LDACS wireless link protocol stack defines two layers, the physical layer and the data link layer.

7.3. LDACS Physical Layer

The physical layer provides the means to transfer data over the radio channel. The LDACS GS supports bi-directional links to multiple aircraft under its control. The forward link direction (FL; G2A) and the reverse link direction (RL; A2G) are separated by frequency division duplex. Forward link and reverse link use a 500 kHz channel each. The ground-station transmits a continuous stream of Orthogonal Frequency-Division Multiplexing (OFDM) symbols on the forward link. In the reverse link different aircraft are separated in time and frequency using a combination of Orthogonal Frequency-Division Multiple-Access (OFDMA) and Time-Division Multiple-Access (TDMA). Aircraft thus transmit discontinuously on the reverse link with radio bursts sent in precisely defined transmission opportunities allocated by the ground-station.

7.4. LDACS Data Link Layer

The data-link layer provides the necessary protocols to facilitate concurrent and reliable data transfer for multiple users. The LDACS data link layer is organized in two sub-layers: The medium access sub-layer and the logical link control sub-layer. The medium access sub-layer manages the organization of transmission opportunities in slots of time and frequency. The logical link control sub-layer provides acknowledged point-to-point logical channels between the aircraft and the ground-station using an automatic repeat request protocol. LDACS supports also unacknowledged point-to-point channels and G2A broadcast.

7.5. LDACS Mobility

LDACS supports layer 2 handovers to different LDACS channels. Handovers may be initiated by the aircraft (break-before-make) or by the GS (make-before-break). Make-before-break handovers are only supported for ground-stations connected to the same GSC.

External handovers between non-connected LDACS sub-networks or different aeronautical data links shall be handled by the FCI multi-link concept.

8. Reliability and Availability

8.1. Layer 2

LDACS has been designed with applications related to the safety and regularity of flight in mind. It has therefore been designed as a deterministic wireless data link (as far as this is possible).

Based on channel measurements of the L-band channel [SCHN2016] and respecting the specific nature of the area of application, LDACS was designed from the PHY layer up with robustness in mind.

In order to maximize the capacity per channel and to optimally use the available spectrum, LDACS was designed as an OFDM-based FDD system, supporting simultaneous transmissions in Forward Link (FL; G2A) and Reverse Link (RL; A2G). The legacy systems already deployed in the L-band limit the bandwidth of both channels to approximately 500 kHz.

The LDACS physical layer design includes propagation guard times sufficient for the operation at a maximum distance of 200 nautical miles from the GS. In actual deployment, LDACS can be configured for any range up to this maximum range.

The LDACS FL physical layer is a continuous OFDM transmission. LDACS RL transmission is based on OFDMA-TDMA bursts, with silence between such bursts. The RL resources (i.e. bursts) are assigned to different users (ASs) on demand by the ground station (GS).

The LDACS physical layer supports adaptive coding and modulation for user data. Control data is always encoded with the most robust coding and modulation (QPSK coding rate 1/2).

LDACS medium access on top of the physical layer uses a static frame structure to support deterministic timer management. As shown in figure 3 and 4, LDACS framing structure is based on Super-Frames (SF) of 240ms duration corresponding to 2000 OFDM symbols. FL and RL boundaries are aligned in time (from the GS perspective) allowing for deterministic sending windows for KEEP ALIVE messages and control and data channels in general.

LDACS medium access is always under the control of the GS of a radio cell. Any medium access for the transmission of user data has to be requested with a resource request message stating the requested

amount of resources and class of service. The GS performs resource scheduling on the basis of these requests and grants resources with resource allocation messages. Resource request and allocation messages are exchanged over dedicated contention-free control channels.

The purpose of QoS in LDACS medium access is to provide prioritized medium access at the bottleneck (the wireless link). The signaling of higher layer QoS requirements to LDACS is yet to be defined. A DiffServ-based solution with a small number of priorities is to be expected.

LDACS has two mechanisms to request resources from the scheduler in the GS.

Resources can either be requested "on demand" with a given priority. On the forward link, this is done locally in the GS, on the reverse link a dedicated contention-free control channel is used called Dedicated Control Channel (DCCH; roughly 83 bit every 60 ms). A resource allocation is always announced in the control channel of the forward link (Common Control Channel (CCCH); variably sized). Due to the spacing of the reverse link control channels every 60 ms, a medium access delay in the same order of magnitude is to be expected.

Resources can also be requested "permanently". The permanent resource request mechanism supports requesting recurring resources in given time intervals. A permanent resource request has to be canceled by the user (or by the ground-station, which is always in control).

User data transmissions over LDACS are therefore always scheduled by the GS, while control data uses statically (i.e. at cell entry) allocated recurring resources (DCCH and CCCH). The current specification specifies no scheduling algorithm. Scheduling of reverse link resources is done in physical Protocol Data Units (PDU) of 112 bit (or larger if more aggressive coding and modulation is used). Scheduling on the forward link is done Byte- wise since the forward link is transmitted continuously by the GS.

In addition to having full control over resource scheduling, the GS can send forced Handover (HO) commands for off-loading or RF channel management, e.g. when the signal quality declines and a more suitable GS is in the AS reach. With robust resource management of the capacities of the radio channel, reliability and robustness measures are therefore also anchored in the LDACS management entity.

In addition, to radio resource management, the LDACS control channels are also used to send keep-alive messages, when they are not otherwise used. Since the framing of the control channels is deterministic, missing keep-alive messages can thus be immediately detected. This information is made available to the multi-link protocols for fault management.

The protocol used to communicate faults is not defined in the LDACS specification. It is assumed that vendors would use industry standard protocols like the Simple Network Management Protocol or the Network Configuration Protocol where security permits.

The LDACS data link layer protocol running on top of the medium access sub-layer uses ARQ to provide reliable data transmission on layer 2.

It employs selective repeat ARQ with transparent fragmentation and reassembly to the resource allocation size to achieve low latency and a low overhead without losing reliability. It ensures correct order of packet delivery without duplicates. In case of transmission errors it identifies lost fragments with deterministic timers synced to the medium access frame structure and initiates retransmission. Additionally, the priority mechanism of LDACS ensures the timely delivery of messages with high importance.

8.2. Beyond Layer 2

LDACS availability can be increased by appropriately deploying LDACS infrastructure: This means proliferating the number of terrestrial base stations. However, the scarcity of aeronautical spectrum for data link communication (in the case of LDACS: tens of MHz in the L-band) and the long range (in the case of LDACS: up to 400 km) make this quite hard. The deployment of a larger number of small cells is certainly possible, suffers, however, also from the scarcity of spectrum. An additional constraint to take into account, is that Distance Measuring Equipment (DME) is the primary user of the aeronautical L-band. That is, any LDACS deployment has to take DME frequency planning into account, too.

The aeronautical community has therefore decided not to rely on a single communication system or frequency band. It is envisioned to have multiple independent data link technologies in the aircraft (e.g. terrestrial and SatCom) in addition to legacy VHF voice.

However, as of now no reliability and availability mechanisms that could utilize the multi-link have been specified on Layer 3 and above.

Below Layer 2 aeronautics usually relies on hardware redundancy. To protect availability of the LDACS link, an aircraft equipped with LDACS will have access to two L-band antennae with triple redundant radio systems as required for any safety relevant system by ICAO.

9. Protocol Stack

The protocol stack of LDACS is implemented in the AS, GS, and GSC: It consists of the Physical Layer (PHY) with five major functional blocks above it. Four are placed in the Data Link Layer (DLL) of the AS and GS: (1) Medium Access Layer (MAC), (2) Voice Interface (VI), (3) Data Link Service (DLS), (4) LDACS Management Entity (LME). The last entity resides within the Sub-Network Layer: Sub-Network Protocol (SNP). The LDACS network is externally connected to voice units, radio control units, and the ATN Network Layer.

Figure 4 shows the protocol stack of LDACS as implemented in the AS and GS.

```
            IPv6                    Network Layer
             |
             |
   +------------------+  +-----+
   |        SNP       |--|     |   Sub-Network
```

```
   |                  |  |    |   Layer
   +------------------+  |    |
             |           | LME|
   +------------------+  |    |
   |       DLS        |  |    |   Logical Link
   |                  |  |    |   Control Layer
   +------------------+  +----+
             |             |
            DCH         DCCH/CCCH
             |          RACH/BCCH
             |             |
   +--------------------------+
   |          MAC             |   Medium Access
   |                          |   Layer
   +--------------------------+
                |
   +--------------------------+
   |          PHY             |   Physical Layer
   +--------------------------+
                |
                |
              ((*))
              FL/RL            radio channels
                                 separated by FDD
```

Figure 4: LDACS protocol stack in AS and GS

9.1. Medium Access Control (MAC) Entity Services

The MAC time framing service provides the frame structure necessary to realize slot-based Time Division Multiplex (TDM) access on the physical link. It provides the functions for the synchronization of the MAC framing structure and the PHY Layer framing. The MAC time framing provides a dedicated time slot for each logical channel.

The MAC Sub-Layer offers access to the physical channel to its service users. Channel access is provided through transparent logical channels. The MAC Sub-Layer maps logical channels onto the appropriate slots and manages the access to these channels. Logical channels are used as interface between the MAC and LLC Sub-Layers.

The LDACS framing structure for FL and RL is based on Super-Frames (SF) of 240 ms duration. Each SF corresponds to 2000 OFDM symbols. The FL and RL SF boundaries are aligned in time (from the view of the GS).

In the FL, an SF contains a Broadcast Frame of duration 6.72 ms (56 OFDM symbols) for the Broadcast Control Channel (BCCH), and four Multi-Frames (MF), each of duration 58.32 ms (486 OFDM symbols).

In the RL, each SF starts with a Random Access (RA) slot of length 6.72 ms with two opportunities for sending reverse link random access frames for the Random Access Channel (RACH), followed by four MFs. These MFs have the same fixed duration of 58.32 ms as in the FL, but a different internal structure

Figure 5 and Figure 6 illustrates the LDACS frame structure.

```
^
|     +------+------------+------------+------------+------------+
|  FL | BCCH |     MF     |     MF     |     MF     |     MF     |
F     +------+------------+------------+------------+------------+
r     <---------------- Super-Frame (SF) - 240ms ---------------->
e
q     +------+------------+------------+------------+------------+
u  RL | RACH |     MF     |     MF     |     MF     |     MF     |
e     +------+------------+------------+------------+------------+
n     <---------------- Super-Frame (SF) - 240ms ---------------->
c
y
|
----------------------------- Time ------------------------------>
|
```

Figure 5: LDACS super-frame structure

```
   ^
   |     +-------------+------+-------------+
   |  FL |     DCH     | CCCH |     DCH     |
   F     +-------------+------+-------------+
   r     <---- Multi-Frame (MF) - 58.32ms -->
   e
   q     +------+---------------------------+
   u  RL | DCCH |             DCH           |
   e     +------+---------------------------+
   n     <---- Multi-Frame (MF) - 58.32ms -->
   c
   y
   |
   ----------------------------- Time ------------------------------>
   |
```

Figure 6: LDACS multi-frame (MF) structure

9.2. Data Link Service (DLS) Entity Services

The DLS provides acknowledged and unacknowledged (including broadcast and packet mode voice) bi-directional exchange of user data. If user data is transmitted using the acknowledged data link service, the sending DLS entity will wait for an acknowledgement from the receiver. If no acknowledgement is received within a specified time frame, the sender may automatically try to retransmit its data. However, after a certain number of failed retries, the sender will suspend further retransmission attempts and inform its client of the failure.

The data link service uses the logical channels provided by the MAC:

1. A ground-stations announces its existence and access parameters in the Broadcast Channel (BC).
2. The Random Access Channel (RA) enables AS to request access to an LDACS cell.
3. In the Forward Link (FL) the Common Control Channel (CCCH) is used by the GS to grant access to data channel resources.
4. The reverse direction is covered by the Reverse Link (RL), where aircraft-stations need to request resources before sending. This happens via the Dedicated Common Control Channel (DCCH).

5. User data itself is communicated in the Data Channel (DCH) on the FL and RL.

9.3. Voice Interface (VI) Services

The VI provides support for virtual voice circuits. Voice circuits may either be set-up permanently by the GS (e.g., to emulate voice party line) or may be created on demand. The creation and selection of voice circuits is performed in the LME. The VI provides only the transmission services.

9.4. LDACS Management Entity (LME) Services

The mobility management service in the LME provides support for registration and de-registration (cell entry and cell exit), scanning RF channels of neighboring cells and handover between cells. In addition, it manages the addressing of aircraft/ ASs within cells. It is controlled by the network management service in the GSC.

The resource management service provides link maintenance (power, frequency and time adjustments), support for adaptive coding and modulation (ACM), and resource allocation.

9.5. Sub-Network Protocol (SNP) Services

The data link service provides functions required for the transfer of user plane data and control plane data over the LDACS sub-network.

The security service provides functions for secure communication over the LDACS sub-network. Note that the SNP security service applies cryptographic measures as configured by the ground station controller.

10. Security Considerations

10.1. Reasons for Wireless Digital Aeronautical Communications

Aviation will require secure exchanges of data and voice messages for managing the air-traffic flow safely through the airspaces all over the world. Historically Communication Navigation Surveillance (CNS) wireless communications technology emerged from military and a threat landscape where inferior technological and financial capabilities of adversaries were assumed [STR2016]. The main communication method for ATC today is still an open analogue voice broadcast within the aeronautical VHF band. Currently, the information security is purely procedural based by using well-trained personnel and proven communications procedures. This communication method has been in service since 1948. However since the emergence of civil aeronautical CNS application and today, the world has changed. First of all civil applications have significant lower spectrum available than military applications. This means several military defense

mechanisms such as frequency hopping or pilot symbol scrambling and thus a defense-in-depth approach starting at the physical layer is impossible for civil systems. With the rise of cheap Software Defined Radios (SDR), the previously existing financial barrier is almost gone and open source projects such as GNU radio [GNU2012] allow the new type of unsophisticated listeners and possible attackers. Furthermore most CNS technology developed in ICAO relies on open standards, thus syntax and semantics of wireless digital aeronautical communications can be common knowledge for attackers. Finally with increased digitization and automation of civil aviation the human as control instance is being taken gradually out of the loop. Autonomous transport drones or single piloted aircraft demonstrate this trend. However without profound cybersecurity measures such as authenticity and integrity checks of messages in-transit on the wireless link or mutual entity authentication, this lack of a control instance can prove disastrous. Thus future digital communications waveforms will need additional embedded security features to fulfill modern information security requirements like authentication and integrity. However, these security features require sufficient bandwidth which is beyond the capabilities of a VHF narrowband communications system. For voice and data communications, sufficient data throughput capability is needed to support the security functions while not degrading performance. LDACS is a data link technology with sufficient bandwidth to incorporate security without losing too much user throughput.

As digitalization progresses even further with LDACS and automated procedures such as 4D-Trajectories allowing semi-automated en-route flying of aircraft, LDACS requires stronger cybersecurity measures.

10.2. Requirements for LDACS

Overall there are several business goals for cybersecurity to protect in future communication infrastructure in civil aviation:

1. Safety: The system must sufficiently mitigate attacks, which contribute to safety hazards.
2. Flight regularity: The system must sufficiently mitigate attacks, which contribute to delays, diversions, or cancellations of flights.
3. Protection of business interests: The system must sufficiently mitigate attacks which result in financial loss, reputation damage, disclosure of sensitive proprietary information, or disclosure of personal information.

To further analyze assets and derive threats and thus protection scenarios several Threat-and Risk Analysis were performed for LDACS [MAE20181] , [MAE20191]. These results allowed deriving security scope and objectives from the requirements and the conducted Threat-and Risk Analysis.

10.3. Security Objectives for LDACS

Security considerations for LDACS are defined by the official ICAO SARPS [ICA2018]:

1. LDACS shall provide a capability to protect the availability and continuity of the system.
2. LDACS shall provide a capability including cryptographic mechanisms to protect the integrity of messages in transit.
3. LDACS shall provide a capability to ensure the authenticity of messages in transit.
4. LDACS should provide a capability for nonrepudiation of origin for messages in transit.
5. LDACS should provide a capability to protect the confidentiality of messages in transit.

6. LDACS shall provide an authentication capability.
7. LDACS shall provide a capability to authorize the permitted actions of users of the system and to deny actions that are not explicitly authorized.
8. If LDACS provides interfaces to multiple domains, LDACS shall provide capability to prevent the propagation of intrusions within LDACS domains and towards external domains.

10.4. Security Functions for LDACS

These objectives were used to derive several security functions for LDACS required to be integrated in the LDACS cybersecurity architecture: (1) Identification, (2) Authentication, (3) Authorization, (4) Confidentiality, (5) System Integrity, (6) Data Integrity, (7) Robustness, (8) Reliability, (9) Availability, and (10) Key and Trust Management. Several works investigated possible measures to implement these security functions [BIL2017], [MAE20181], [MAE20191]. Having identified security requirements, objectives and functions now we must look at the scope of the applicability of these functions.

10.5. Security Architectural Details for LDACS

With requirements out of the way, we want to have a look at the scope of the LDACS security model. This includes looking at the entities, identification, authentication and authorization of entities, integrity, authenticity and confidentiality of data in-transit and more.

10.5.1. Entities in LDACS Security Model

First of all the question is what entities do we have in a simplified LDACS architectural model: Network operators such as the Societe Internationale de Telecommunications Aeronautiques (SITA) [SIT2020] and ARINC [ARI2020] are providing access to the (1) Ground IPS network via an (2) A2G LDACS Router. This router is attached to a closed off LDACS Access Network (3) which connects via further (4) Access Routers to the different (5) LDACS Cell Ranges, each controlled by a (6) Ground Station Controller (GSC) and spanning a local LDACS Access Network connecting to the (7) Ground Stations (GS) that serve one LDACS cell. Via the (8) A2G wireless LDACS data link (9) Airborne Stations (AS) the aircraft is connected to the ground network and via the (10) airborne voice interface and (11) airborne network interface, airborne data can be sent via the AS back to the GS and the forwarded back via GSC, LDACS local access network, access routers, LDACS access network, A2G LDACS router to the ground IPS network.

10.5.2. Matter of LDACS Entity Identification

Each entity described in the sections above must be uniquely identified within the LDACS network thus we need LDACS specific identities for (1) the Aircraft Station (AS), (2) Ground Station (GS), (3) Ground Station Controller (GSC) and (4) Network Operator (NO). The aircraft itself can be identified using the ICAO unique address of an aircraft, the call sign of that aircraft or the recently founded Privacy ICAO Address (PIA) program [FAA2020]. It is conceivable that the LDACS AS will use a combination of aircraft identification, radio component identification such as MAC addresses and even operator features identification to create a unique AS LDACS identification tag. Similar to a 4G's eNodeB Serving Network (SN) Identification tag, a GS could be identified using a similar field. And again similar to 4G's Mobility Management Entities (MME), a GSC could be identified using similar identification fields within the LDACS network. The identification of the network operator is again similar to 4G (e.g., E-Plus, AT&T, TELUS, ...), in the way that the aeronautical network operators are listed (e.g., ARINC [ARI2020] and SITA [SIT2020]).

10.5.3. Matter of LDACS Entity Authentication and Key Negotiation

In order to anchor Trust within the system all LDACS entities connected to the ground IPS network shall be rooted in an LDACS specific chain-of-trust and PKI solution, quite similar to AeroMACS approach [CRO2016]. These X.509 certificates [RFC5280] residing at the entities and incorporated in the LDACS PKI proof the ownership of their respective public key, include information about the identity of the owner and the digital signature of the entity that has verified the certificate's content. First all ground infrastructures must mutually authenticate to each other, negotiate and derive keys and thus secure all ground connections. How this process is handled in detail is still an ongoing discussion. However, established methods to secure user plane by IPSec [RFC4301] and IKEv2 [RFC7296] or the application layer via TLS 1.3 [RFC8446] are conceivable. The LDACS PKI with their chain-of-trust approach, digital certificates and public entity keys lay the groundwork for this step. In a second step the aircraft with the LDACS radio (AS) approaches an LDACS cell and performs a cell entry with the corresponding groundstation (GS). Similar to the LTE cell attachment process [TS33.401], where authentication happens after basic communication has been enabled between AS and GS (step 5a in the UE attachment process [TS33.401]), the next step is mutual authentication and key exchange. Thus in step three using the identity based Station-to-Station (STS) protocol with Diffie-Hellman Key Exchange [MAE2020], AS and GS establish mutual trust by authenticating each other, exchanging key material and finally both ending up with derived key material. A key confirmation is mandatory before the communication channel AS-GS can be opened for user-data communications.

10.5.4. Matter of LDACS Message-in-transit Confidentiality, Integrity and Authenticity

The subsequent key material from the previous step can then be used to protect LDACS Layer 2 communications via applying encryption and integrity protection measures on the SNP layer of the LDACS protocol stack. As LDACS transports AOC and ATS data, the integrity of that data is most important, while confidentiality only needs to be applied to AOC data to protect business interests [ICA2018]. This possibility of providing low layered confidentiality and integrity protection ensures a secure delivery of user data over the air gap. Furthermore it ensures integrity protection of LDACS control data.

10.6. Security Architecture for LDACS

Summing up all previous paragraphs, a draft of the cybersecurity architecture of LDACS can be found in [ICA2018], [MAE20182] and updates in [MAE20191], [MAE20192], [MAE2020]. It proposes the use of an own LDACS PKI, identity management based on aircraft identities and network operator identities (e.g., SITA and ARINC), public key certificates incorporated in the PKI based chain-of-trust and stored in the entities allowing for mutual authentication and key exchange procedures, key derivation mechanisms for perfect forward secrecy and user/control plane message-in-transit integrity and confidentiality protection. This secures data traveling over the airgap between aircraft and groundstation and also between groundstation and Air Navigation Service Provider regardless of the secure or unsecure nature of application data. Of course application data itself must be additionally secured to achieve end-to-end security (secure dialogue service), however the LDACS datalinks aims to provide an additional layer of protection just for this network segment.

11. Privacy Considerations

LDACS provides a Quality of Service (QoS), and the generic considerations for such mechanisms apply.

12. IANA Considerations

This memo includes no request to IANA.

13. Acknowledgements

Thanks to all contributors to the development of LDACS and ICAO PT-T.

Thanks to Klaus-Peter Hauf, Bart Van Den Einden, and Pierluigi Fantappie for further input to this draft.

Thanks to SBA Research Vienna for fruitful discussions on aeronautical communications concerning security incentives for industry and potential economic spillovers.

14. Normative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

15. Informative References

[SCHN2016] Schneckenburger, N., Jost, T., Shutin, D., Walter, M., Thiasiriphet, T., Schnell, M., and U.C. Fiebig, "Measurement of the L-band Air-to-Ground Channel for Positioning Applications", IEEE Transactions on Aerospace and Electronic Systems, 52(5), pp.2281-229 , 2016.

[MAE20191] Maeurer, N., Graeupl, T., and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation", IEEE 38th Digital Avionics Systems Conference (DACS), pp. 1-10, San Diego, CA, USA , 2019.

[MAE20192] Maeurer, N. and C. Schmitt, "Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis", IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-13, Herndon, VA, USA , 2019.

[GRA2019] Graeupl, T., Rihacek, C., and B. Haindl, "LDACS A/G Specification", SESAR2020 PJ14-02-01 D3.3.030 , 2019.

[FAN2019] Pierattelli, S., Fantappie, P., Tamalet, S., van den Einden, B., Rihacek, C., and T. Graeupl, "LDACS Deployment Options and Recommendations", SESAR2020 PJ14-02-01 D3.4.020 , 2019.

[MAE20182] Maeurer, N. and A. Bilzhause, "A Cybersecurity

Architecture for the L-band Digital Aeronautical Communications System (LDACS)", IEEE 37th Digital Avionics Systems Conference (DASC), pp. 1-10, London, UK , 2017.

[GRA2011] Graeupl, T. and M. Ehammer, "L-DACS1 Data Link Layer Evolution of ATN/IPS", 30th IEEE/AIAA Digital Avionics Systems Conference (DASC), pp. 1-28, Seattle, WA, USA , 2011.

[GRA2018] Graeupl, T., Schneckenburger, N., Jost, T., Schnell, M., Filip, A., Bellido-Manganell, M.A., Mielke, D.M., Maeurer, N., Kumar, R., Osechas, O., and G. Battista, "L-band Digital Aeronautical Communications System (LDACS) flight trials in the national German project MICONAV", Integrated Communications, Navigation, Surveillance Conference (ICNS), pp. 1-7, Herndon, VA, USA , 2018.

[SCH20191] Schnell, M., "DLR Tests Digital Communications Technologies Combined with Additional Navigation Functions for the First Time", 2019.

[ICA2018] International Civil Aviation Organization (ICAO), "L-Band Digital Aeronautical Communication System (LDACS)", International Standards and Recommended Practices Annex 10 - Aeronautical Telecommunications, Vol. III - Communication Systems , 2018.

[SAJ2014] Haindl, B., Meser, J., Sajatovic, M., Mueller, S., Arthaber, H., Faseth, T., and M. Zaisberger, "LDACS1 Conformance and Compatibility Assessment", IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), pp. 1-11, Colorado Springs, CO, USA , 2014.

[RIH2018] Rihacek, C., Haindl, B., Fantappie, P., Pierattelli, S., Graeupl, T., Schnell, M., and N. Fistas, "L-band Digital Aeronautical Communications System (LDACS) Activities in SESAR2020", Integrated Communications Navigation and Surveillance Conference (ICNS), pp. 1-8, Herndon, VA, USA , 2018.

[BEL2019] Bellido-Manganell, M. A. and M. Schnell, "Towards Modern Air-to-Air Communications: the LDACS A2A Mode", IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), pp. 1-10, San Diego, CA, USA , 2019.

[TS33.401] Zhang, D., "3GPP System Architecture Evolution (SAE); Security architecture", T33.401, 3GPP , 2012.

[CRO2016] Crowe, B., "Proposed AeroMACS PKI Specification is a Model for Global and National Aeronautical PKI Deployments", WiMAX Forum at 16th Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-19, New York, NY, USA , 2016.

[MAE2020] Maeurer, N., Graeupl, T., and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS", IEEE/AIAA 39th Digital Avionics Systems Conference (DASC), pp. 1-10, San Antonio, TX, USA , 2020.

[STR2016] Strohmeier, M., Schaefer, M., Pinheiro, R., Lenders, V., and I. Martinovic, "On Perception and Reality in Wireless Air Traffic Communication Security", IEEE Transactions on Intelligent Transportation Systems, 18(6), pp. 1338-1357, New York, NY, USA , 2016.

[BIL2017] Bilzhause, A., Belgacem, B., Mostafa, M., and T. Graeupl, "Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management", IEEE Aerospace and Electronic Systems Magazine, 32(11), pp. 22-33, New York, NY, USA , 2017.

[MAE20181] Maeurer, N. and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis", IEEE Integrated Communications, Navigation, Surveillance Conference (ICNS), pp. 1-11, New York, NY, USA , 2018.

[FAA2020] FAA, "Federal Aviation Administration. ADS-B Privacy.", August 2020, <https://www.faa.gov/nextgen/equipadsb/privacy/>.

[GNU2012] GNU Radio project, "GNU radio", August 2012, <http://gnuradio.org>.

[SIT2020] SITA, "Societe Internationale de Telecommunications Aeronautiques", August 2020, <https://www.sita.aero/>.

[ARI2020] ARINC, "Aeronautical Radio Incorporated", August 2020, <https://www.aviation-ia.com/>.

[DO350A] RTCA SC-214, "Safety and Performance Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)", May 2016, <https://standards.globalspec.com/std/10003192/rtca-do-350-volume-1-2>.

[RAW-TECHNOS]
Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-thubert-raw-technologies-05, 18 May 2020, <https://tools.ietf.org/html/draft-thubert-raw-technologies-05>.

[RAW-USE-CASES]
Papadopoulos, G., Thubert, P., Theoleyre, F., and C. Bernardos, "RAW use cases", Work in Progress, Internet-Draft, draft-bernardos-raw-use-cases-04, 13 July 2020, <https://tools.ietf.org/html/draft-bernardos-raw-use-cases-04>.

Authors' Addresses

Nils Maeurer (editor)
German Aerospace Center (DLR)
Muenchner Strasse 20
82234 Wessling
Germany

Email: Nils.Maeurer@dlr.de

Thomas Graeupl (editor)
German Aerospace Center (DLR)
Muenchner Strasse 20
82234 Wessling
Germany

Email: Thomas.Graeupl@dlr.de

Corinna Schmitt (editor)
Research Institute CODE, UniBwM
Werner-Heisenberg-Weg 28
85577 Neubiberg
Germany

Email: corinna.schmitt@unibw.de