RAW
Internet-Draft
Intended status: Informational
Expires: 25 April 2022

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

22 October 2021

L-band Digital Aeronautical Communications System (LDACS)
draft-ietf-raw-ldacs-09

Abstract

This document gives 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 provides a data link for IPv6 network-based aircraft guidance. High reliability and availability for IP connectivity over LDACS, as well as security, 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 25 April 2022.

Table of Contents

1. Introduction

One of the main pillars of the modern Air Traffic Management (ATM) system is the existence of a communications infrastructure that enables efficient aircraft control and safe aircraft separation in all phases of flight. Current systems are technically mature but suffering from the Very High Frequency (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 communications infrastructure.

This modernization is realized in two steps: (1) the transition of communications datalinks from analogue to digital technologies and, (2) the introduction of IPv6 based networking protocols in aeronautical networks [RFC4291], [RFC7136], [ICAO2015].

Step (1) is realized via ATM communications transitioning from analogue VHF voice [KAMA2010] to more spectrum efficient digital data communication. For terrestrial communications the European ATM Master Plan foresees this transition to be realized by the development of the L-band Digital Aeronautical Communications System (LDACS). Since central Europe has been identified as the area of the world, that suffers the most from increased saturation of the VHF band, the initial roll-out of LDACS will likely start there, and continue to other increasingly saturated zones as the east- and west-cost of the US and parts of Asia [ICAO2018].

Technically LDACS enables IPv6 based air- ground communication related to aviation safety and regularity of flight [ICAO2015]. Passenger communication and similar services are not supported, since only communications related to "safety and regularity of flight" are permitted in protected aviation frequency bands. The particular challenge is that no additional frequencies 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 protected frequency band. Since LDACS will be used for aircraft guidance, high reliability and availability for IP connectivity over LDACS are essential.

Step (2) is a strategy for the worldwide roll-out of IPv6 capable digital aeronautical inter-networking. This is called the Aeronautical Telecommunications Network (ATN)/Internet Protocol Suite (IPS) (hence, ATN/IPS). It is specified in the International Civil Aviation Organization (ICAO) document Doc 9896 [ICAO2015], the Radio Technical Commission for Aeronautics (RTCA) document DO-379 [RTCA2019], the European Organization for Civil Aviation Equipment (EUROCAE) document ED-262 [EURO2019], and the Aeronautical Radio Incorporated (ARINC) document P858 [ARI2021]. LDACS is subject to these regulations since it provides access subnets to the ATN/IPS.

ICAO has chosen IPv6 as basis for the ATN/IPS mostly for historical reasons, since a previous architecture based on ISO/OSI protocols, the ATN/OSI, failed in the market place.

In the context of safety-related communications, LDACS will play a major role in future ATM. ATN/IPS datalinks will provide diversified terrestrial and space-based connectivity in a multi-link concept, called the Future Communications Infrastructure (FCI) [VIR2021]. From a technical point of view the FCI will realize airborne multi-homed IPv6 networks connected to a global ground network via at least two independent communication technologies. This is considered in more detail in related IETF work in progress [I-D.haindl-lisp-gb-atn] [I-D.ietf-rtgwg-atn-bgp].

In the context of WG-RAW, developing options, such as intelligent switching between datalinks, for reliably delivering content from and to endpoints, is foreseen. As LDACS is part of such a concept, the work of RAW is immediately applicable. In general, with the aeronautical communications system transitioning to ATN/IPS, and data being transported via IPv6, closer cooperation and collaboration between the aeronautical and IETF community is desirable.

LDACS standardization within the framework of ICAO started in December 2016. The ICAO standardization group has produced an initial Standards and Recommended Practices (SARPS) document [ICA2018]. It 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 encourages cooperation between the aeronautical and the IETF community.

2. Terminology

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

A/A Air/Air
A/G Air/Ground
A2G Air-to-Ground
ACARS Aircraft Communications Addressing and Reporting System
ADS-B Automatic Dependent Surveillance - Broadcast
ADS-C Automatic Dependent Surveillance - Contract
AeroMACS Aeronautical Mobile Airport Communications System
ANSP Air Traffic Network Service Provider
AOC Aeronautical Operational Control
AR Access Router
ARINC Aeronautical Radio, Incorporated
ARQ Automatic Repeat reQuest
AS Aircraft Station
ATC Air Traffic Control
ATM Air Traffic Management
ATN Aeronautical Telecommunication Network
ATS Air Traffic Service
BCCH Broadcast Channel
CCCH Common Control Channel
CM Context Management
CNS Communication Navigation Surveillance
COTS Commercial Off-The-Shelf
CPDLC Controller Pilot Data Link Communications
CRL Certificate Revocation List
CSP Communications Service Provider
DCCH Dedicated Control Channel
DCH Data Channel
DiffServ Differentiated Services
DLL Data Link Layer
DLS Data Link Service
DME Distance Measuring Equipment
DSB-AM Double Side-Band Amplitude Modulation
DTLS Datagram Transport Layer Security
EUROCAE European Organization for Civil Aviation Equipment

FAA Federal Aviation Administration
FCI Future Communications Infrastructure
FDD Frequency Division Duplex
FL Forward Link
GANP Global Air Navigation Plan
GBAS Ground Based Augmentation System
GNSS Global Navigation Satellite System
GS Ground-Station
G2A Ground-to-Air
HF High Frequency
ICAO International Civil Aviation Organization
IP Internet Protocol
IPS Internet Protocol Suite
kbit/s kilobit per second
LDACS L-band Digital Aeronautical Communications System
LLC Logical Link Control
LME LDACS Management Entity
MAC Medium Access Control
MF Multi Frame
OFDM Orthogonal Frequency-Division Multiplexing
OFDMA Orthogonal Frequency-Division Multiplexing Access
OSI Open Systems Interconnection
PHY Physical Layer
QPSK Quadrature Phase-Shift Keying
RACH Random Access Channel
RL Reverse Link
RTCA Radio Technical Commission for Aeronautics
SARPS Standards and Recommended Practices
SDR Software Defined Radio
SESAR Single European Sky ATM Research
SF Super-Frame
SNP Sub-Network Protocol
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) services via voice and data communications systems through all phases of flight. ATC refers to communication for flight guidance. AOC is a generic term referring to the business communication of airlines. It refers to the mostly proprietary exchange of data between the aircraft of the airline, its operation centers, and its service partners. ARINC document 633 was developed and first released in 2007 [ARI2019] with the goal to standardize these messages for interoperability, e.g., messages

between the airline and fueling or de-icing companies. 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 complements 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/Ground (A/G) and Air/Air (A/A) communications. The communications equipment is either ground-based working in the High Frequency (HF) or VHF frequency band or satellite-based. All VHF and HF voice communications are operated via open broadcast channels without authentication, encryption or other protective measures. The use of well-proven communications procedures via broadcast channels can help to enhance the safety of communications. 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 and satellite communications for remote and oceanic regions. 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 are 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 ATM applications, such as flight-centric operation with point-to-point communications between pilots and air traffic control officers. [BOE2019]

3.2. Data Communications Today

Like for voice, data communications into the cockpit, are 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 the order of kilobits per second. While the aircraft is on ground, some additional communications systems are available, like the Aeronautical Mobile Airport Communications System (AeroMACS) or public cellular networks, operating in the Airport (APT) domain and able to deliver broadband communications capability. [BOE2019]

The data communications networks, used for the transmission of data relating to the safety and regularity of 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 and 4D trajectory negotiations. [BOE2019]

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 [MAE20211] [BEL2021]. 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 (GNAP). [BOE2019]

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 these 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].

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 have 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 FCI. The FCI will support quality of service, diversity, and mobility under the umbrella of the "multi-link concept". This work is led 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] [MAE20211] [BEL2021].

5. Applicability

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

LDACS supports communications 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 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, not yet provided in contemporarily deployed aeronautical communications systems.

5.1.1. Priorities

LDACS is able to manage service priorities, an important feature not available in some of the current data link deployments. Thus, LDACS guarantees bandwidth availability, 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 Air traffic Network Service Providers (ANSP). This includes concepts for key and trust management, mutual authentication and key establishment protocols, key derivation measures, user and control message-in-transit protection, secure logging and availability and robustness measures [MAE20182] [MAE2021].

5.1.3. High Data Rates

The user data rate of LDACS is 315 kbit/s to 1428 kbit/s on the Forward Link (FL) for the Ground-to-Air (G2A) connection, and 294 kbit/s to 1390 kbit/s on the Reverse Link (RL) for the Air-to-Ground (A2G) connection, depending on coding and modulation. This is up to two orders of magnitude greater than current terrestrial digital aeronautical communications systems, such as the VHF Data Link mode 2 (VDLm2), provide [ICAO2019] [GRA2019].

5.2. Application

LDACS will be used by several aeronautical applications ranging from enhanced communications protocol stacks (multi-homed mobile IPv6 networks in the aircraft and potentially ad-hoc networks between aircraft) to broadcast communication applications (sending Ground Based Augmentation System (GBAS) correction data) and integration with other service domains (using the communications signal for navigation) [MAE20211].

5.2.1. Air/Ground Multilink

It is expected that LDACS, together with upgraded satellite-based communications systems, will be deployed within the 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 will be realized by multi-homed mobile IPv6 networks in the aircraft. The related protocol stack is currently under development by ICAO, within SESAR, and the IETF [I-D.haindl-lisp-gb-atn] [I-D.ietf-rtgwg-atn-bgp].

5.2.2. Air/Air Extension for LDACS

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

Direct A/A communication between aircraft in terms of ad-hoc data networks are currently considered a research topic since there is no immediate operational need for it, although several possible use cases are discussed (Automatic Dependent Surveillance - Broadcast (ADS-B), 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 A/A is currently not part of the standardization process and will not be covered within this document.

5.2.3. Flight Guidance

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

1. Context Management (CM): The CM application manages 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 Communications (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 takes over most of the communication currently performed over VHF voice and enables new services that do not lend themselves to voice communication (i.e., 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 for implementing in-flight trajectory management.

CM, CPDLC, and ADS-C are available on legacy datalinks, but are 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 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 aircraft’s 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 [MAE20211].

5.2.4. Business Communications of Airlines

In addition to air traffic services, AOC services are transmitted over LDACS. AOC is a generic term referring to the business communication of airlines, between the airlines and service partners on the ground and their own aircraft in the air. Regulatory-wise, this is considered related to safety and regularity of flight and may therefore be transmitted over LDACS. AOC communication is considered the main business case for LDACS communications service providers since modern aircraft generate significant amounts of data (i.e., engine maintenance data).

5.2.5. LDACS-based Navigation

Beyond communications, radio signals can always also be used for navigation. This fact is used for the LDACS navigation concept.

For future aeronautical navigation, ICAO recommends the further development of GNSS based technologies as primary means for navigation. Due to the large separation between navigational satellites and aircraft, the power of the GNSS signals received by the aircraft is, however, 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 solutions consists of exploiting the built-in navigation capabilities of LDACS operation. That is, the normal operation of LDACS for ATC and AOC communications would also directly enable the aircraft to navigate and obtain a reliable timing reference from the LDACS GSs.

LDACS navigation has already been demonstrated in practice in two flight measurement campaigns [SHU2013] [BEL2021] [MAE20211]. .

6. Requirements

The requirements for LDACS are mostly defined by its application area: Communications 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 ATN are therefore expected to remain in service for decades. The VDLm2 data link currently used for digital terrestrial internetworking was developed in the 1990ies (the use of the Open Systems Interconnection (OSI) stack indicates that as well). VDLm2 is expected to be used at least for several decades. In this respect aeronautical communications (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 Aircraft Communications Addressing and Reporting System (ACARS) or the OSI stack. The objective of the development effort of LDACS, as part of the FCI, is to replace legacy OSI stack 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 versions of Ethernet 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 do not provide sufficient bandwidth (i.e., with VDLm2 currently in the order of 10 kbit/s). 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 addressing 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 like Voice-over-IP) at the gateway connecting the LDACS network to other aeronautical ground networks (i.e., the ATN). On the avionics side, in the aircraft, aviation specific solutions are to be expected.

In addition to these 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 Communications Service Provider (CSP) scope.

Continuity, availability, and integrity requirements are defined in [DO350A] volume 1 Table 5-14, and Table 6-13. Appendix A presents the required information.

In a similar vein, requirements to fault management are defined in the same tables.

7. Characteristics

LDACS will become one of several wireless access networks connecting aircraft to the ATN implemented by the FCI.

The current LDACS design is focused on the specification of layer one and two. However, for the purpose of this work, only layer two details are discussed here.

Achieving the stringent 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) and several GS, each of them providing one LDACS radio cell.

User plane interconnection to the ATN is facilitated by the AR peering with an A/G Router connected to the ATN.

The internal control plane of an LDACS sub-network interconnects the GSs. An LDACS sub-network is illustrated in Figure 1.

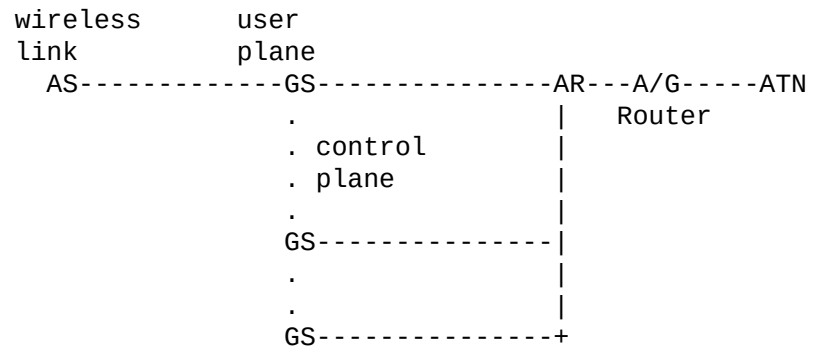

Figure 1: LDACS sub-network with three GSs and one AS

7.2. Topology

LDACS is a cellular point-to-multipoint system. It 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 A/G communications within its cell. The LDACS GS can simultaneously support multiple bi-directional communications to the ASs under its control. LDACS's GSs themselves are connected to each other and the AR.

Prior to utilizing the system an aircraft 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.

7.3. LDACS Protocol Stack

The protocol stack of LDACS is implemented in the AS and GS: 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 Control (MAC) Layer, (2) Voice Interface (VI), (3) Data Link Service (DLS), and (4) LDACS Management Entity (LME). The last entity resides within the sub-network layer: the Sub-Network Protocol (SNP). The LDACS network is externally connected to voice units, radio control units, and the ATN network layer.

LDACS is considered an ATN/IPS radio access technology, from the view of ICAO's regulatory framework. Hence, the interface between ATN and LDACS must be IPv6 based, as regulatory documents, such as ICAO Doc 9896 [ICAO2015] and DO-379 [RTCA2019] clearly foresee that. The translation between IPv6 layer and SNP layer is currently subject of ongoing standardization efforts and at the time of writing not finished yet.

Figure 2 shows the protocol stack of LDACS as implemented in the AS and GS. Acronyms used here are introduced throughout the upcoming sections.

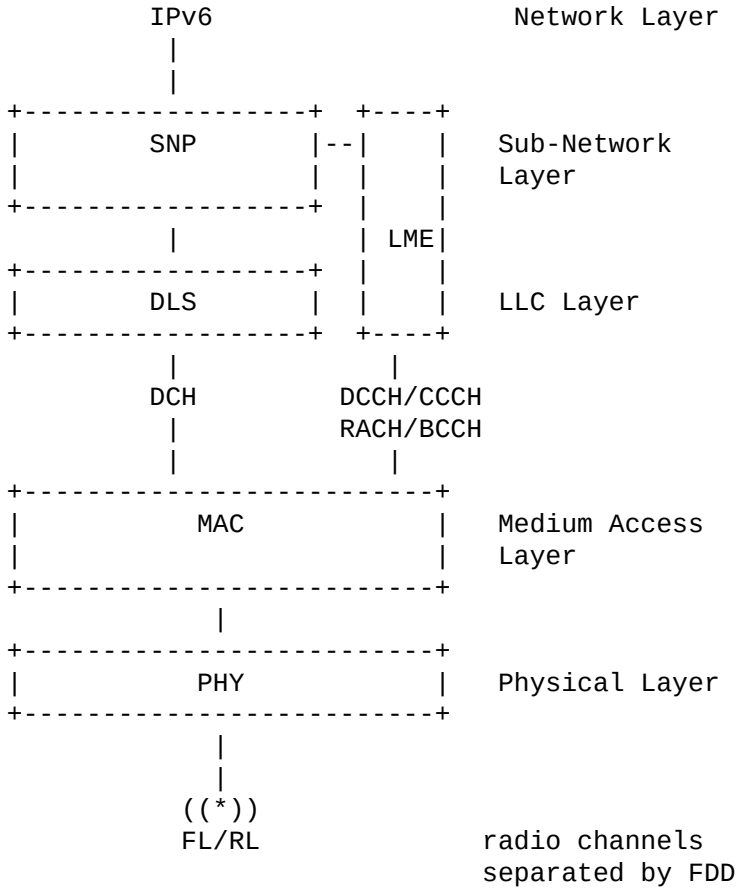

Figure 2: LDACS protocol stack in AS and GS

7.3.1. 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 FL direction at the G2A connection and the RL direction at the A2G connection are separated by Frequency Division Duplex (FDD). FL and RL use a 500 kHz channel each. The GS transmits a continuous stream of Orthogonal Frequency-Division Multiplexing Access (OFDM) symbols on the FL. In the RL different aircraft are separated in time and frequency using Orthogonal Frequency-Division Multiple Access (OFDMA). Aircraft thus transmit discontinuously on the RL via short radio bursts sent in precisely defined transmission opportunities allocated by the GS.

7.3.2. 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 (LLC) sub-layer. The medium access sub-layer manages the organization of transmission opportunities in slots of time and frequency. The LLC sub-layer provides acknowledged point-to-point logical channels between the aircraft and the GS using an Automatic Repeat reQuest (ARQ) protocol. LDACS supports also unacknowledged point-to-point channels and G2A Broadcast transmission.

7.3.2.1. Medium Access Control (MAC) Services

The MAC time framing service provides the frame structure necessary to realize slot-based time-division multiplex-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.

7.3.2.2. Data Link Service (DLS) 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 DLS, 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 DLS uses the logical channels provided by the MAC:

1. A GS announces its existence and access parameters in the Broadcast Channel (BCCH).
2. The Random Access Channel (RACH) enables AS to request access to an LDACS cell.
3. In the 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 RL, where ASs need to request resources before sending. This happens via the Dedicated Control Channel (DCCH).
5. User data itself is communicated in the Data Channel (DCH) on the FL and RL.

Access to the FL and RL data channel is granted by the scheduling mechanism implemented in the LME discussed below.

7.3.2.3. 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.

7.3.2.4. 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 within cells.

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

The resource management service accepts resource requests from/for different AS and issues resource allocations accordingly. While the scheduling algorithm is not specified and a point of possible vendor differentiation, it is subject to the following requirements:

1. Resource scheduling must provide channel access according to the priority of the request
2. Resource scheduling must support "one-time" requests.
3. Resource scheduling must support "permanent" requests that reserve a resource until the request is canceled e.g. for digital voice circuits.

7.3.3. LDACS Sub-Network Layer and Protocol Services

Lastly, the SNP handles the transition from IPv6 packts to LDACS internal packet structures. This work is ongoing and not part of this document. The DLS 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 user data communication over the LDACS sub-network. Note that the SNP security service applies cryptographic measures as configured by the GS.

7.4. LDACS Mobility

LDACS supports layer 2 handovers to different LDACS cells. Handovers may be initiated by the aircraft (break-before-make) or by the GS (make-before-break). Make-before-break handovers are only supported between GSs connected to each other.

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

8. Reliability and Availability

8.1. Below Layer 1

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 aeronautical systems by ICAO.

8.2. Layer 1 and 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 LDACS was designed from the PHY layer up with robustness in mind. Channel measurements of the L-band channel [SCH2016] confirmed LDACS to be well adapted to its channel.

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 FL in the G2A connection and RL in the A2G connection. 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 physical layer supports adaptive coding and modulation for user data. Control data is always encoded with the most robust coding and modulation (FL: Quadrature Phase-Shift Keying (QPSK), coding rate 1/2, RL: QPSK, coding rate 1/3).

LDACS medium access layer on top of the physical layer uses a static frame structure to support deterministic timer management. As shown in Figure 3 and Figure 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 slots for control and data channels. This initial AS time synchronization and time synchronization maintenance is based on observing the synchronization symbol pairs that repetitively occur within the FL stream, being sent by the controlling GS [GRA2019].

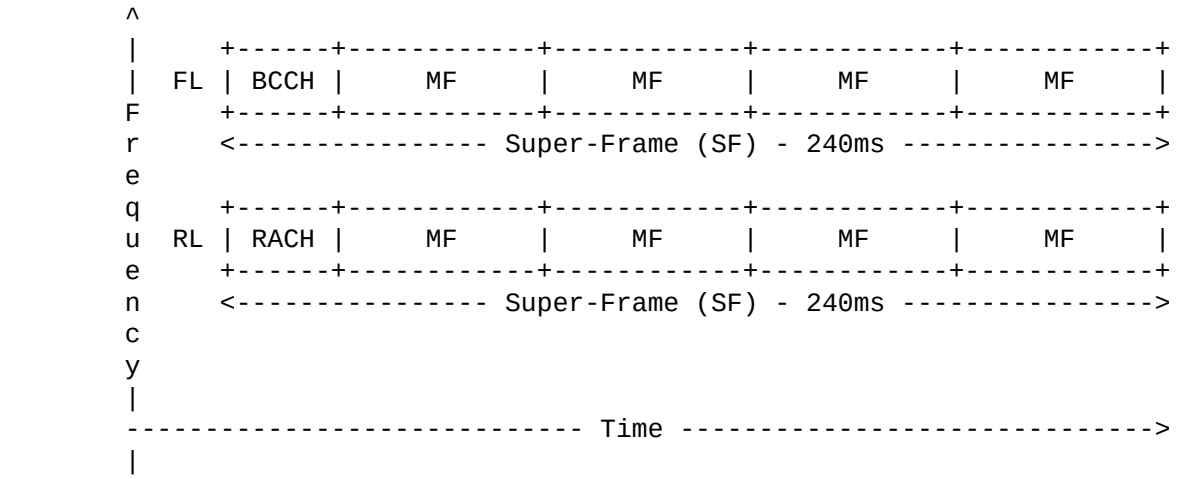

Figure 3: SF structure for LDACS

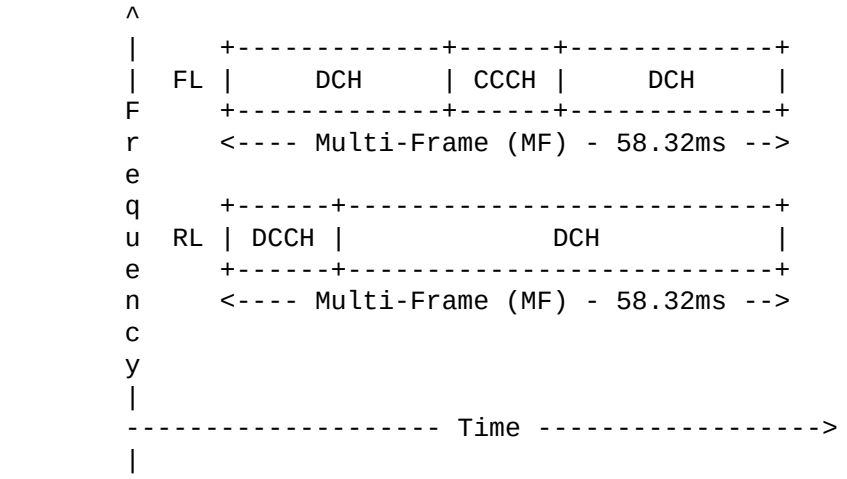

Figure 4: MF structure for LDACS

LDACS cell entry is conducted with an initial control message exchange via the RACH and the BCCH.

After cell entry, LDACS medium access is always under the control of the GS of a radio cell. Any medium access for the transmission of user data on a DCH 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 (DCCH and CCCH).

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

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

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 the data channel.

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.

8.3. Beyond Layer 2

LDACS availability can be increased by appropriately deploying LDACS infrastructure: This means proliferating the number of terrestrial ground 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 200 nautical miles) 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 consider, 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.

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 satellite communications) in addition to legacy VHF voice.

However, as of now, no reliability and availability mechanisms that could utilize the multi-link architecture, have been specified on Layer 3 and above. Even if LDACS has been designed for reliability, the wireless medium presents significant challenges to achieve deterministic properties such as low packet error rate, bounded consecutive losses, and bounded latency. Support for high reliability and availability for IP connectivity over LDACS is therefore, highly desirable, needs, however, to be adapted to the specific use case.

9. Security

ICAO Doc 9896 foresees transport layer security [ICAO2015] for all aeronautical data as described in ARINC P858 [ARI2021], most likely realized via Datagram Transport Layer Security (DTLS) [RFC6012] [RFC6347].

LDACS also needs to comply with in-depth security requirements, stated in P858, for the radio access technologies transporting ATN/IPS data [ARI2021]. These requirements imply that LDACS must provide layer 2 security in addition to any higher layer mechanisms.

9.1. Security in 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 communications method for ATC today is still an open analogue voice broadcast within the aeronautical VHF band. Currently, information security is mainly 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 applications in the 70s, and today, the world has changed.

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 infeasible for civil systems. With the rise of cheap Software Defined Radios (SDRs), the previously existing financial barrier is almost gone and open source projects such as GNU radio [GNU2021] allow a new type of unsophisticated listeners and possible attackers.

Most CNS technology developed in ICAO relies on open standards, thus syntax and semantics of wireless digital aeronautical communications should be expected to be common knowledge for attackers. 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. These security features require sufficient bandwidth which is beyond the capabilities of currently deployed VHF narrowband communications systems. 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 data throughput.

9.2. LDACS Requirements

Overall, there are several business goals for cybersecurity to protect, within the FCI 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 analyses were performed for LDACS [MAE20181] , [MAE20191]. These results allowed deriving security scope and objectives from the requirements and the conducted threat- and risk analysis.

9.3. LDACS Security Objectives

Security considerations for LDACS are defined by the official SARPS document by ICAO [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.

Currently, a change request for these SARPS aims to limit the "non-repudiation of origin of messages in transit" requirement only to the authentication and key establishment messages at the beginning of every session.

9.4. LDACS Security Functions

These objectives were used to derive several security functions for LDACS required to be integrated in the LDACS cybersecurity architecture: Identification, Authentication, Authorization, Confidentiality, System Integrity, Data Integrity, Robustness, Reliability, Availability, and Key and Trust Management. Several works investigated possible measures to implement these security functions [BIL2017], [MAE20181], [MAE20191].

9.5. LDACS Security Architecture

The requirements lead to a LDACS security model, including different entities for identification, authentication and authorization purposes, ensuring integrity, authenticity and confidentiality of data. A draft of the cybersecurity architecture of LDACS can be found in [ICA2018] and [MAE20182] and respective updates in [MAE20191], [MAE20192], [MAE2020], and most recently [MAE2021].

9.5.1. Entities

A simplified LDACS architectural model requires the following entities: Network operators such as the Societe Internationale de Telecommunications Aeronautiques (SITA) [SIT2020] and ARINC [ARI2020] are providing access to the ground IPS network via an A/G LDACS router. This router is attached to a closed off LDACS access network, which connects via further (access routers to the different LDACS cell ranges, each controlled by a GS (serving one LDACS cell), with several interconnected GS spanning a local LDACS access network. Via the A/G wireless LDACS data link AS the aircraft is connected to the ground network and via the aircraft’s VI and aircraft’s network interface, aircraft’s data can be sent via the AS back to the GS, then to the LDACS local access network, access routers, LDACS access network, A/G LDACS router and finally to the ground IPS network [ICAO2015].

9.5.2. Entity Identification

LDACS needs specific identities for the AS, the GS, and the network operator. 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 of the Federal Aviation Administration (FAA) program with the same name [FAA2020]. It is conceivable that the LDACS AS will use a combination of aircraft identification, radio component identification and even operator feature identification to create a unique AS LDACS identification tag. Similar to a 4G's eNodeB serving network identification tag, a GS could be identified using a similar field. The identification of the network operator is again similar to 4G (e.g., E-Plus, AT&T, and TELUS), in the way that the aeronautical network operators are listed (e.g., ARINC [ARI2020] and SITA [SIT2020]).

9.5.3. Entity Authentication and Key Establishment

In order to anchor trust within the system, all LDACS entities connected to the ground IPS network will be rooted in an LDACS specific chain-of-trust and PKI solution, quite similar to AeroMACS's approach [CRO2016]. These certificates, residing at the entities and incorporated in the LDACS PKI, providing 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 AS with the LDACS radio aboard, approaches an LDACS cell and performs a cell-attachment procedure with the corresponding GS. This procedure consists of (1) the basic cell entry [GRA2019] and (2) a Mutual Authentication and Key Establishment (MAKE) procedure [MAE2021].

Note, that LDACS will foresee multiple security levels. To address the issue of the long service life of LDACS (i.e., possibly >30 years) and the security of current pre-quantum cryptography, these security levels include pre- and post-quantum cryptographic solutions. Limiting security data on the LDACS datalink as much as possible, to reserve as much space for actual user data transmission, is key in the LDACS security architecture, this is also reflected in the underlying cryptography: Pre-quantum solutions will rely on elliptic curves [KOB1987], while post-quantum solutions consider

Falcon [SON2021] [MAE2021] or similar lightweight PQC signature schemes, and SIKE or SABER as key establishment options [SIK2021] [ROY2020].

9.5.4. Message-in-transit Confidentiality, Integrity and Authenticity

The 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. IANA Considerations

This memo includes no request to IANA.

11. 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 the Chair for Network Security and the research institute CODE for their comments and improvements.

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

Thanks to the Aeronautical Communications group at the Institute of Communications and Navigation of the German Aerospace Center (DLR). With that, the authors would like to explicitly thank Miguel Angel Bellido-Manganell and Lukas Marcel Schalk for their thorough feedback.

12. Normative References

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

[ICAO2015] International Civil Aviation Organization (ICAO), "Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, Doc 9896", January 2015, <https://standards.globalspec.com/std/10026940/icao-9896>.

[RTCA2019] Radio Technical Commission for Aeronautics (RTCA), "Internet Protocol Suite Profiles, DO-379", September 2019, <https://www.rtca.org/products/do-379/>.

[EURO2019] European Organization for Civil Aviation Equipment (EUROCAE), "Technical Standard of Aviation Profiles for ATN/IPS, ED-262", September 2019, <https://eshop.eurocae.net/eurocae-documents-and-reports/ed-262/>.

[ARI2021] ARINC, "Internet Protocol Suite (IPS) For Aeronautical Safety Services Part 1- Airborne IP System Technical Requirements, ARINC SPECIFICATION 858 P1", June 2021, <https://standards.globalspec.com/std/14391274/858p1>.

13. Informative References

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, DOI 10.17487/RFC3610, September 2003, <https://www.rfc-editor.org/info/rfc3610>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[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>.

[RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", RFC 4493, DOI 10.17487/RFC4493, June 2006, <https://www.rfc-editor.org/info/rfc4493>.

[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>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, DOI 10.17487/RFC6012, October 2010, <https://www.rfc-editor.org/info/rfc6012>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

[RFC7236] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Authentication Scheme Registrations", RFC 7236, DOI 10.17487/RFC7236, June 2014, <https://www.rfc-editor.org/info/rfc7236>.

[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>.

[SCH2016] 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.

[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.

[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/>.

[GNU2021] GNU Radio project, "GNU radio", October 2021, <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>.

[ICAO2019] International Civil Aviation Organization (ICAO), "Manual on VHF Digital Link (VDL) Mode 2, Doc 9776", January 2019, <https://store.icao.int/en/manual-on-vhf-digital-link-vdl-mode-2-doc-9776>.

[KAMA2010] Kamali, B., "An Overview of VHF Civil Radio Network and the Resolution of Spectrum Depletion", Integrated Communications, Navigation, and Surveillance Conference, pp. F4-1-F4-8 , May 2010.

[SON2021] Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M., and R. Karri, "FALCON", Hardware Architectures for Post-Quantum Digital Signature Schemes, pp. 31-41 , November 2021.

[KOB1987] Koblitz, N. and M. Hellman, "Elliptic Curve Cryptosystems", Mathematics of Computation, 48(177):203-209. , January 1987.

[SIK2021] SIKE, "SIKE â Supersingular Isogeny Key Encapsulation", October 2021, <https://sike.org/>.

[ROY2020] Roy, S.S.. and A. Basso, "High-Speed Instruction-Set Coprocessor For Lattice-Based Key Encapsulation Mechanism: Saber In Hardware", IACR Transactions on Cryptographic Hardware and Embedded Systems, 443-466. , August 2020.

[RAW-TECHNOS] Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-ietf-raw-technologies-04, 3 August 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-raw-technologies-04>.

[RAW-USE-CASES] Papadopoulos, G. Z., Thubert, P., Theoleyre, F., and C. J. Bernardos, "RAW use cases", Work in Progress, Internet-Draft, draft-ietf-raw-use-cases-03, 20 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-raw-use-cases-03>.

[I-D.haindl-lisp-gb-atn]
Haindl, B., Lindner, M., Rahman, R., Comeras, M. P., Moreno, V., Maino, F., and B. Venkatachalapathy, "Ground-Based LISP for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-haindl-lisp-gb-atn-06, 6 March 2021, <https://datatracker.ietf.org/doc/html/draft-haindl-lisp-gb-atn-06>.

[I-D.ietf-rtgwg-atn-bgp]
Templin, F. L., Saccone, G., Dawra, G., Lindem, A., and V. Moreno, "A Simple BGP-based Mobile Routing System for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-ietf-rtgwg-atn-bgp-11, 6 July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-rtgwg-atn-bgp-11>.

[ICAO2018] International Civil Aviation Organization (ICAO), "Handbook on Radio Frequency Spectrum Requirements for Civil Aviation, Doc 9718, Volume 1, ICAO Spectrum Strategy, Policy Statements and Related Information", July 2018, <https://www.icao.int/safety/FSMP/Documents/Doc9718/Doc9718_Vol_I_2nd_ed_(2018)corr1.pdf>.

[EURO2021] European Organization for Civil Aviation Equipment (EUROCAE), "Radio Frequency Function 2020 report", March 2021, <https://www.eurocontrol.int/>.

[ARI2019] ARINC, "AOC Air-Ground Data And Message Exchange Format, ARINC 633", January 2019, <https://standards.globalspec.com/std/13152055/ARINC%20633>.

[VIR2021] Virdia, A., Stea, G., and G. Dini, "SAPIENT: Enabling Real-Time Monitoring and Control in the Future Communication Infrastructure of Air Traffic Management", IEEE Transactions on Intelligent Transportation Systems, 22(8):4864-4875 , August 2021.

[SHU2013] Shutin, D., Schneckenburger, N., Walter, M., and M. Schnell, "LDACS1 Ranging Performance - An Analysis Of Flight Measurement Results", IEEE 32th Digital Avionics Systems Conference (DASC), pp. 1-10, East Syracuse, NY, USA , October 2013.

[BEL2021] Bellido-Manganell, M.A., Graeupl, T., Heirich, O., Maeurer, N., Filip-Dhaubhadel, A., Mielke, D.M., Schalk, L.M., Becker, D., Schneckenburger, N., and M. Schnell,

"LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System", IEEE Transactions on Aerospace and Electronic Systems, pp. 1-19 , September 2021.

[MAE2021] Maeurer, N., Graeupl, T., Gentsch, C., Guggemos, T., Tiepelt, M., Schmitt, C., and G. Dreo Rodosek, "A Secure Cell-Attachment Procedure for LDACS", 1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS), pp. 1-10, Vienna, Austria , September 2021.

[MAE20211] Maeurer, N., Graeupl, T., Bellido-Manganell, M.A., Mielke, D.M., Filip-Dhaubhadel, A., Heirich, O., Gerberth, D., Flux, M., Schalk, L.M., Becker, D., Schneckenburger, N., and M. Schnell, "Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communications System (LDACS)", IEEE Aerospace and Electronic Systems Magazine, 36(4), pp. 8-17 , April 2021.

[BOE2019] Boegl, T., Rautenberg, M., Haindl, R., Rihacek, C., Meser, J., Fantappie, P., Pringvanich, N., Micallef, J., Klauspeter, H.., MacBride, J., Sacre, P., v.d. Eiden, B., Graeupl, T., and M. Schnell, "LDACS White Paper - A Roll-out Scenario", International Civil Aviation Organization, Communications Panel - Data Communications Infrastructure Working Group - Third Meeting, pp. 1-8, Montreal, Canada , October 2019.

Appendix A. Selected Information from DO-350A

This appendix includes the continuity, availability, and integrity requirements applicable for LDACS defined in [DO350A].

The following terms are used here:

CPDLC Controller Pilot Data Link Communication
DT Delivery Time (nominal) value for RSP
ET Expiration Time value for RCP
FH Flight Hour
MA Monitoring and Alerting criteria
OT Overdue Delivery Time value for RSP
RCP Required Communication Performance
RSP Required Surveillance Performance
TT Transaction Time (nominal) value for RCP

	RCP 130	RCP 130
Parameter	ET	TT95%
Transaction Time (sec)	130	67
Continuity	0.999	0.95
Availability	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH

Table 1: CPDLC Requirements for RCP 130

	RCP 240	RCP 240	RCP 400	RCP 400
Parameter	ET	TT95%	ET	TT95%
Transaction Time (sec)	240	210	400	350
Continuity	0.999	0.95	0.999	0.95
Availability	0.989 (safety)	0.989 (efficiency)	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH

Table 2: CPDLC Requirements for RCP 240/400

RCP Monitoring and Alerting Criteria in case of CPDLC:

- 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.

	RSP 160	RSP 160	RSP 180	RSP 180	RSP 400	RSP 400
Parameter	OT	DT95%	OT	DT95%	OT	DT95%
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	0.989 (safety)	0.989 (efficiency)	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH

Table 3: ADS-C Requirements

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.

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