
Stream: Internet Engineering Task Force (IETF)
RFC: [9372](#)
Category: Informational
Published: March 2023
ISSN: 2070-1721
Authors: N. Mäurer, Ed. T. Gräupl, Ed.
German Aerospace Center (DLR) *German Aerospace Center (DLR)*
C. Schmitt, Ed.
Research Institute CODE, UniBwM

RFC 9372

L-Band Digital Aeronautical Communications System (LDACS)

Abstract

This document gives an overview of the L-band Digital Aeronautical Communications System (LDACS) architecture, which provides a secure, scalable, and spectrum-efficient terrestrial data link for civil aviation. LDACS is a scheduled and reliable multi-application cellular broadband system with support for IPv6. It is part of a larger shift of flight guidance communication moving to IP-based communication. High reliability and availability of IP connectivity over LDACS, as well as security, are therefore essential. The intent of this document is to introduce LDACS to the IETF community, raise awareness on related activities inside and outside of the IETF, and to seek expertise in shaping the shift of aeronautics to IP.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc9372>.

Copyright Notice

Copyright (c) 2023 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Acronyms	5
3. Motivation and Use Cases	7
3.1. Voice Communications Today	7
3.2. Data Communications Today	8
4. Provenance and Documents	8
5. Applicability	9
5.1. Advances beyond the State of the Art	9
5.1.1. Priorities	10
5.1.2. Security	10
5.1.3. High Data Rates	10
5.2. Application	10
5.2.1. Air/Ground Multilink	10
5.2.2. Air/Air Extension for LDACS	11
5.2.3. Flight Guidance	11
5.2.4. Business Communications of Airlines	12
5.2.5. LDACS-Based Navigation	12
6. Requirements	13
7. Characteristics	14
7.1. LDACS Access Network	14
7.2. Topology	15
7.3. LDACS Protocol Stack	15
7.3.1. LDACS Physical Layer	16
7.3.2. LDACS Data Link Layer	16

7.3.3. LDACS Subnetwork Layer and Protocol Services	18
7.4. LDACS Mobility	18
7.5. LDACS Management Interfaces and Protocols	19
8. Reliability and Availability	19
8.1. Below Layer 1	19
8.2. Layers 1 and 2	19
8.3. Beyond Layer 2	21
9. Security Considerations	22
9.1. Security in Wireless Digital Aeronautical Communications	22
9.2. Security in Depth	23
9.3. LDACS Security Requirements	23
9.4. LDACS Security Objectives	24
9.5. LDACS Security Functions	24
9.6. LDACS Security Architecture	24
9.6.1. Entities	24
9.6.2. Entity Identification	25
9.6.3. Entity Authentication and Key Establishment	25
9.6.4. Message-In-Transit Confidentiality, Integrity, and Authenticity	26
9.7. Considerations on LDACS Security Impact on IPv6 Operational Security	26
10. IANA Considerations	26
11. Informative References	26
Appendix A. Selected Information from DO-350A	32
Acknowledgements	34
Authors' Addresses	35

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 they are suffering from the

Very High Frequency (VHF) band's increasing saturation in high-density areas and the limitations posed by analog radio communications. Therefore, aviation strives for a sustainable modernization of the aeronautical communications infrastructure on the basis of IP.

This modernization is realized in two steps: (1) the transition of communications data links from analog to digital technologies and (2) the introduction of IPv6-based networking protocols [RFC8200] in aeronautical networks [ICAO2015].

Step (1) is realized via ATM communications transitioning from analog VHF voice [KAMA2010] to more spectrum-efficient digital data communication. For terrestrial communications, the Global Air Navigation Plan (GANP) created by the International Civil Aviation Organization (ICAO) 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 rollout of LDACS will likely start there and continue to other increasingly saturated zones such as the East and West Coast of the US and parts of Asia [ICAO2018].

Technically, LDACS enables IPv6-based Air/Ground (A/G) 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; thus, it was necessary to develop coexistence mechanisms and procedures to enable the interference-free operation of LDACS in parallel with other aeronautical services and 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.

LDACS is standardized in ICAO and the European Organization for Civil Aviation Equipment (EUROCAE).

This document provides information to the IETF community about the aviation industry transition of flight guidance systems from analog to digital, provides context for LDACS relative to related IETF activities [LISP-GB-ATN], and seeks expertise on realizing reliable IPv6 over LDACS for step (1). This document does not intend to advance LDACS as an IETF Standards Track document.

Step (2) is a strategy for the worldwide rollout of IPv6-capable digital aeronautical internetworking. This is called the Aeronautical Telecommunications Network (ATN) / Internet Protocol Suite (IPS) (hence, ATN/IPS). It is specified in the ICAO document Doc 9896 [ICAO2015], the Radio Technical Commission for Aeronautics (RTCA) document DO-379 [RTCA2019], the EUROCAE document ED-262 [EURO2019], and the Aeronautical Radio Incorporated (ARINC) document 858 [ARI2021]. LDACS is subject to these regulations since it provides an "access network" (link-layer data link) to the ATN/IPS.

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

In the context of safety-related communications, LDACS will play a major role in future ATM. ATN/IPS data links will provide diversified terrestrial and space-based connectivity in a multilink concept called the Future Communications Infrastructure (FCI) [VIR2021]. From a technical point of view, the FCI will realize airborne and multihomed IPv6 networks connected to a global ground network via at least two independent communication technologies. This is considered in more detail in related documents [LISP-GB-ATN] [RTGWG-ATN-BGP]. As such, ICAO has actively sought out the support of IETF to define a mobility solution for step (2), which is currently the Locator/ID Separation Protocol (LISP).

In the context of the Reliable and Available Wireless (RAW) Working Group, developing options, such as intelligent switching between data links, 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. As of 2022, the ICAO standardization group has produced the final Standards and Recommended Practices (SARPS) document [ICAO2022] that defines the general characteristics of LDACS. By the end of 2023, the ICAO standardization group plans to have developed an ICAO technical manual, which is the ICAO equivalent to a technical standard. The LDACS standardization is not finished yet; therefore, this document is a snapshot of the current status. The physical characteristics of an LDACS installation (form, fit, and function) will be standardized by EUROCAE. Generally, the group is open to input from all sources and encourages cooperation between the aeronautical and IETF communities.

2. Acronyms

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
AC-R:	Access Router
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
ARINC:	Aeronautical Radio Incorporated
ARQ:	Automatic Repeat reQuest
AS:	Aircraft Station
ATC:	Air Traffic Control
ATM:	Air Traffic Management

ATN:	Aeronautical Telecommunications 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
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
LISP:	Locator/ID Separation Protocol
LLC:	Logical Link Control
LME:	LDACS Management Entity
MAC:	Medium Access Control
MF:	Multiframe
NETCONF:	Network Configuration Protocol
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
SNMP:	Simple Network Management Protocol
SNP:	Subnetwork 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 and refers to the mostly proprietary exchange of data between the aircraft of the airline and the airline's operation centers and service partners. The 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 and terminal area, connectivity is focused on high bandwidth communications. However, in the en route domain, high reliability, robustness, and range are the main foci. 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 list of 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 can be installed on ground or in the aircraft, in which cases the High Frequency (HF) or VHF frequency band is used. For remote domains, voice communications can also be satellite-based. All VHF and HF voice communications are operated via open Broadcast Channels (BCCHs) without authentication, encryption, or other protective measures. The use of well-proven communications procedures via BCCHs, such as phraseology or read-backs, requiring well-trained personnel help to enhance the safety of communications but does not replace necessary cryptographical security mechanisms. The main voice communications media is still the analog 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. However, this 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 ATC officers [BOE2019].

3.2. Data Communications Today

Like for voice communications, 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 use narrowband radio channels with a data throughput capacity in the order of kbit/s. Additional communications systems are available while the aircraft is on the ground, such as the Aeronautical Mobile Airport Communications System (AeroMACS) or public cellular networks, that operate in the Airport (APT) domain and are able to deliver broadband communications capability [BOE2019].

For regulatory reasons, 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 where the flight crews are supported by narrowband services during flight while passengers have access to in-flight 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 that will be able to provide in-flight broadband services and communications supporting the safety and regularity of flight are under development. In parallel, the ground-based broadband data link technology LDACS is being standardized by ICAO and has recently shown its maturity during flight tests [MAE2021] [BEL2021]. The LDACS technology is scalable, secure, and spectrum-efficient, and it 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 GANP [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 that is able to evolve with aviation needs over the long term. To this end, an LDACS specification has been produced [GRA2020] 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 fulfill the identified requirements [GRA2011].

Up to now, LDACS standardization has been focused on the development of the Physical Layer (PHY) and the Data Link Layer (DLL). Only recently have higher layers come into the focus of the LDACS development activities. Currently no "IPv6 over LDACS" specification is defined; however, SESAR2020 has started experimenting with IPv6-based LDACS and ICAO plans to seek guidance from IETF to develop IPv6 over LDACS. As of May 2022, LDACS defines 1536-byte user data packets [GRA2020] in which IPv6 traffic shall be encapsulated. Additionally, Robust Header Compression (ROHC) [RFC5795] is considered on the LDACS Subnetwork Protocol (SNP) layer (cf. Section 7.3.3).

The IPv6 architecture for the aeronautical telecommunication network is called the ATN/IPS. Link-layer technologies within the ATN/IPS encompass LDACS [GRA2020], AeroMACS [KAMA2018], and several SatCOM candidates; combined with the ATN/IPS, these are called the "FCI". The FCI will support quality of service, link diversity, and mobility under the umbrella of the "multilink concept". The "multilink concept" describes the idea that depending on link quality, communication can be switched seamlessly from one data link technology to another. This work is led by the 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 (ATSS) including ATS-B3 and AOC communications services from deployed Ground-Stations (GSs). The physical layer and data link layer of LDACS are optimized for Controller-Pilot Data Link Communications (CPDLC), but the system also supports digital A/G 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 decoupled 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 will offer several capabilities that are not yet provided in contemporarily deployed aeronautical communications systems. These capabilities were already tested and confirmed in lab or flight trials with available LDACS prototype hardware [BEL2021] [MAE20211].

5.1.1. Priorities

LDACS is able to manage service priorities, which is an important feature that is 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 (ANSPs). This includes concepts for key and trust management, Mutual Authentication and Key Establishment (MAKE) 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 what current terrestrial digital aeronautical communications systems, such as the VHF Data Link mode 2 (VDLm2), provide; see [[ICAO2019](#)] [[GRA2020](#)].

5.2. Application

LDACS will be used by several aeronautical applications ranging from enhanced communications protocol stacks (multihomed mobile IPv6 networks in the aircraft and potentially ad-hoc networks between aircraft) to broadcast communication applications (Global Navigation Satellite System (GNSS) correction data) and integration with other service domains (using the communications signal for navigation) [[MAE20211](#)]. Also, a digital voice service offering better quality and service than current HF and VHF systems is foreseen.

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 that complement each other. Satellite systems are especially 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 hotspots around airports and terminal airspace. In addition, both technologies offer comparable data link capacity; thus, both are well-suited for redundancy, mutual back-up, or load balancing.

Technically, the FCI multilink concept will be realized by multihomed mobile IPv6 networks in the aircraft. The related protocol stack is currently under development by ICAO, within SESAR, and the IETF. Currently, two layers of mobility are foreseen. Local mobility within the LDACS access network is realized through Proxy Mobile IPv6 (PMIPv6), and global mobility between "multilink" access networks (which need not be LDACS) is implemented on top of LISP [[LISP-GB-ATN](#)] [[RFC9300](#)] [[RFC9301](#)].

5.2.2. Air/Air Extension for LDACS

A potential extension of the multilink 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 is 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 a part of the standardization process and will not be covered within this document. However, it is planned that LDACS A/A will be rolled out after the initial deployment of LDACS A/G and seamlessly integrated in the existing LDACS ground-based system.

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 data links 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 the Ground-Based Augmentation System (GBAS) for secure, automated landings. The 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 VHF Data Broadcast (VDB) data link is used. VDB is a narrowband one-way, single-purpose data link without advanced security and is only used to transmit GBAS correction data. These shortcomings show a clear need to replace VDB. A natural candidate to replace it is LDACS, because it is a bidirectional data link, also operates in non-line-of sight scenarios, offers strong integrated link-layer security, and has a considerably larger operational range than VDB [MAE20211].

5.2.4. Business Communications of Airlines

In addition to ATSS, 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; therefore, it may 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 (e.g., engine maintenance data).

5.2.5. LDACS-Based Navigation

Beyond communications, radio signals can always be used for navigation as well. 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. However, due to the large separation between navigational satellites and aircraft, the power of the GNSS signals received by the aircraft 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 such APNT solution is based on 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. Current cell planning for Europe shows 84 LDACS cells to be sufficient [MOST2018] to cover the continent at a sufficient service level. If more than three GSs are visible by the aircraft, via knowing the exact positions of these and having a good channel estimation (which LDACS does due to numerous works mapping the L-band channel characteristics [SCHN2018]), it is possible to calculate the position of the aircraft via measuring signal propagation times to each GS. In flight trials in 2019 with one aircraft (and airborne radio inside it) and just four GSs, navigation feasibility was demonstrated within the footprint of all four GSs with a 95th percentile position-domain error of 171.1m [OSE2019] [BEL2021] [MAE20211]. As such, LDACS can be used independently of GNSS as a navigation alternative. Positioning errors will decrease markedly as more GSs are deployed [OSE2019] [BEL2021] [MAE20211].

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 1990s (the use of the Open Systems Interconnection (OSI) stack indicates that as well). VDLm2 is expected to be used at least for several decades to come. 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 the 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.

Currently, AOC applications 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 (hence the ATN over which only communications related to safety and regularity of flight is handled) and the Internet should be completely separated at Layer 3.

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 operational problems that are currently experienced.

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

In order to fulfill 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 fulfill the requirements defined in RTCA DO-350A/EUROCAE ED-228A [DO350A]. This document defines continuity, availability, and integrity requirements at different scopes for each ATM 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 Volume 1 of [DO350A] in Tables 5-14 and 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 Layers 1 and 2. However, for the purpose of this work, only Layer 2 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 unspecified as of November 2022. Current regulatory documents do not fully specify the above mechanism yet. However, a short overview of the current state shall be given throughout each section here.

7.1. LDACS Access Network

An LDACS access network contains an Access Router (AC-R) and several GSs, each of them providing one LDACS radio cell.

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

The internal control plane of an LDACS access network interconnects the GSs. An LDACS access network is illustrated in [Figure 1](#). Dashes denote the user plane and points denote the control plane.

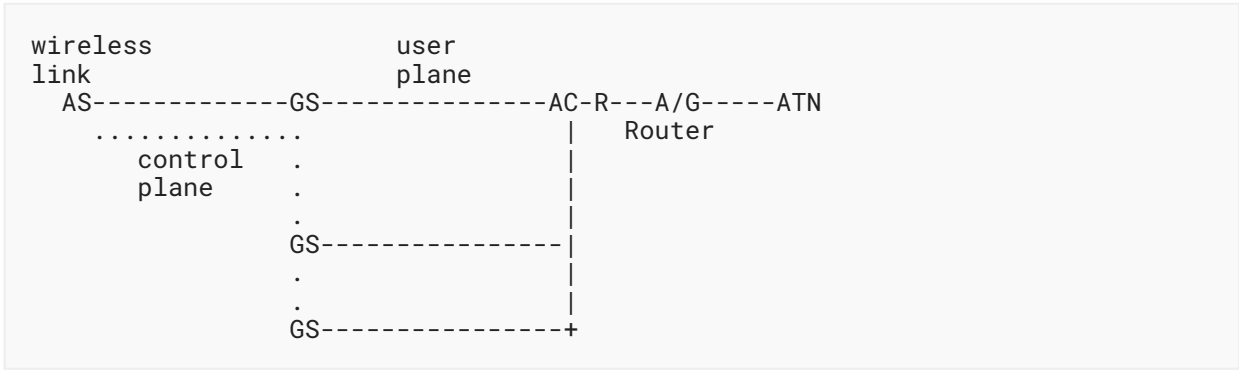


Figure 1: LDACS Access Network with Three GSs and One AS

7.2. Topology

LDACS is a cellular point-to-multipoint system. It assumes a star topology in each cell where Aircraft Stations (ASs) belonging to aircraft within a certain volume of space (the LDACS cell) are 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 bidirectional communications to the ASs under its control. LDACS's GSs themselves are connected to each other and the AC-R.

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 PHY with five major functional blocks above it. Four are placed in the DLL of the AS and GS: Medium Access Control (MAC) layer, Voice Interface (VI), Data Link Service (DLS), and LDACS Management Entity (LME). The fifth entity, the SNP, resides within the subnetwork layer. The LDACS radio is externally connected to a voice unit and radio control unit via the AC-R to the ATN network.

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 the IPv6 layer and SNP layer is currently the subject of ongoing standardization efforts and not finished yet at the time of writing.

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

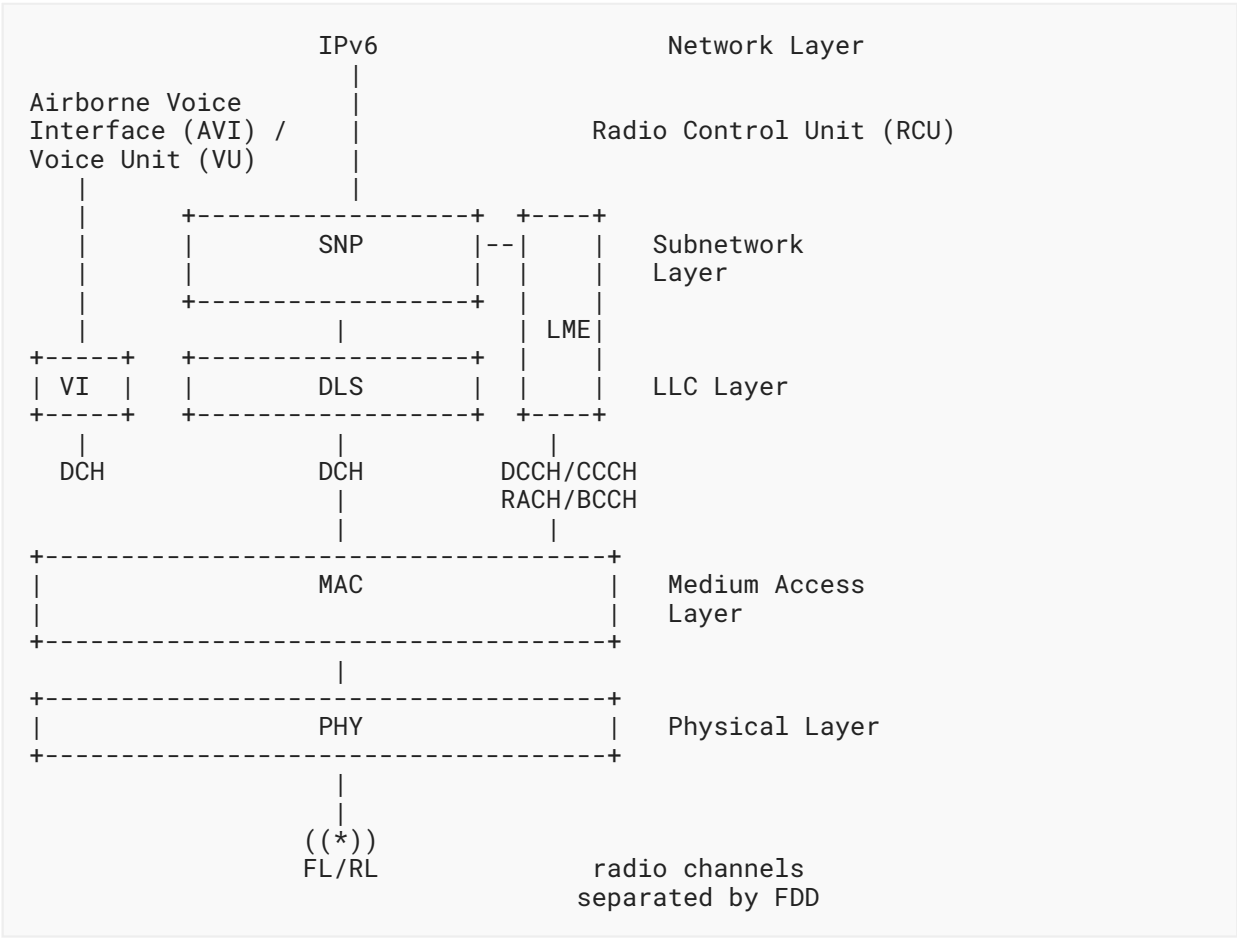


Figure 2: LDACS Protocol Stack in the AS and GS

7.3.1. LDACS Physical Layer

The physical layer provides the means to transfer data over the radio channel. The LDACS GS supports bidirectional 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). Thus, aircraft 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 also supports 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 Services (DLSS)

The DLS provides acknowledged and unacknowledged (including broadcast and packet mode voice) bidirectional 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 the 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 (DCH) 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 DCH on the FL and RL.

Access to the FL and RL DCH 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 be either set up permanently by the GS (e.g., to emulate voice party line) or created on demand.

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 ASs 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 Subnetwork Layer and Protocol Services

Lastly, the SNP layer of LDACS directly interacts with IPv6 traffic. Incoming ATN/IPS IPv6 packets are forwarded over LDACS from and to the aircraft. The final IP addressing structure in an LDACS subnet still needs to be defined; however, the current layout consists of the five network segments: Air Core Net, Air Management Net, Ground Core Net, Ground Management Net, and Ground Net. Any protocols that the ATN/IPS [ICAO2015] defines as mandatory will reach the aircraft; however, listing these here is out of scope. For more information on the technicalities of the above ATN/IPS layer, please refer to [ICAO2015], [RTCA2019], and [ARI2021].

The DLS provides functions that are required for the transfer of user-plane data and control plane data over the LDACS access network. The security service provides functions for secure user data communication over the LDACS access 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 and usually GSs operated by the same service provider.

When a handover between the AS and two interconnected GSs takes place, it can be triggered by the AS or GS. Once that is done, new security information is exchanged between the AS, GS1, and GS2 before the "old" connection is terminated between the AS and GS1 and a "new" connection is set up between the AS and GS2. As a last step, accumulated user data at GS1 is forwarded to GS2 via a ground connection before it is sent via GS2 to the AS. While some information for handover is transmitted in the LDACS DCH, the information remains in the "control plane" part of LDACS and is exchanged between LMEs in the AS, GS1, and GS2. As such, local mobility takes place entirely within the LDACS network and utilizes the PMIPv6 protocol [RFC5213]. The use of PMIPv6 is currently not mandated by standardization and may be vendor-specific. External handovers between non-connected LDACS access networks or different aeronautical data links are handled by the FCI multilink concept.

7.5. LDACS Management Interfaces and Protocols

LDACS management interfaces and protocols are currently not be mandated by standardization. The implementations currently available use SNMP for management and Radius for Authentication, Authorization, and Accounting (AAA). Link state (link up, link down) is reported using the ATN/IPS Aircraft Protocol (AIAP) mandated by ICAO WG-I for multilink.

8. Reliability and Availability

8.1. Below Layer 1

Below Layer 1, aeronautics usually rely 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. Layers 1 and 2

LDACS has been designed with applications related to the safety and regularity of flight in mind; therefore, it has 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 that supports 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 operation at a maximum distance of 200 nautical miles (nm) 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 Figures 3 and 4, LDACS framing structure is based on Super-Frames (SFs) of 240 ms (milliseconds) duration corresponding to 2000 OFDM symbols. OFDM symbol time is 120 microseconds, sampling time is 1.6 microseconds, and guard time is 4.8 microseconds. The structure of an SF is depicted in Figure 3 along with its structure and timings of each part. FL and RL boundaries are aligned in time (from the GS perspective) allowing for deterministic slots for control and DCHs. 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 [GRA2020]. As already mentioned, LDACS data transmission is split into user data (DCH) and control (BCCH and CCCH in FL; RACH and DCCH in RL) as depicted with corresponding timings in Figure 4.

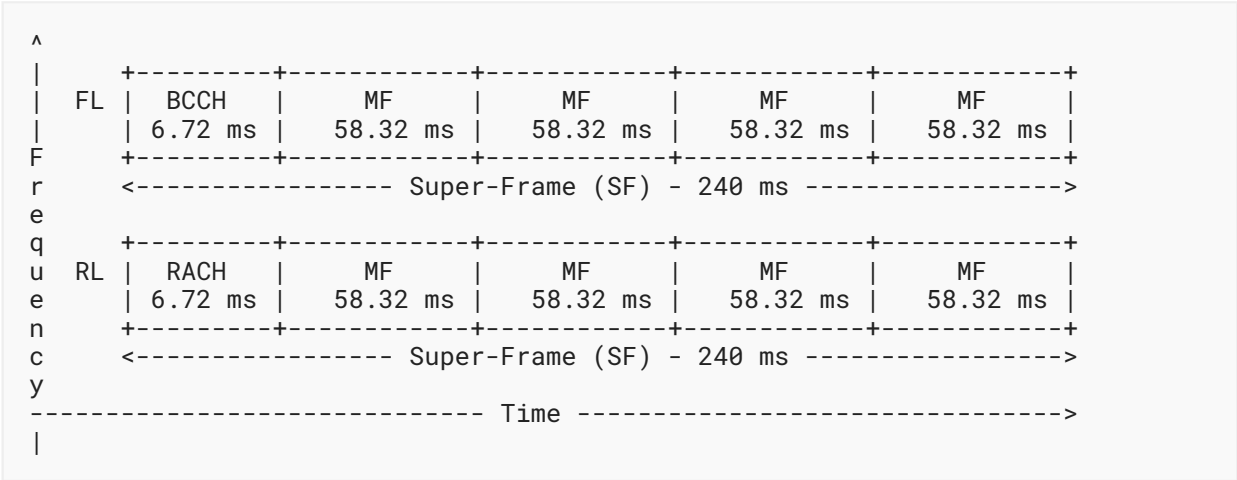


Figure 3: SF Structure for LDACS

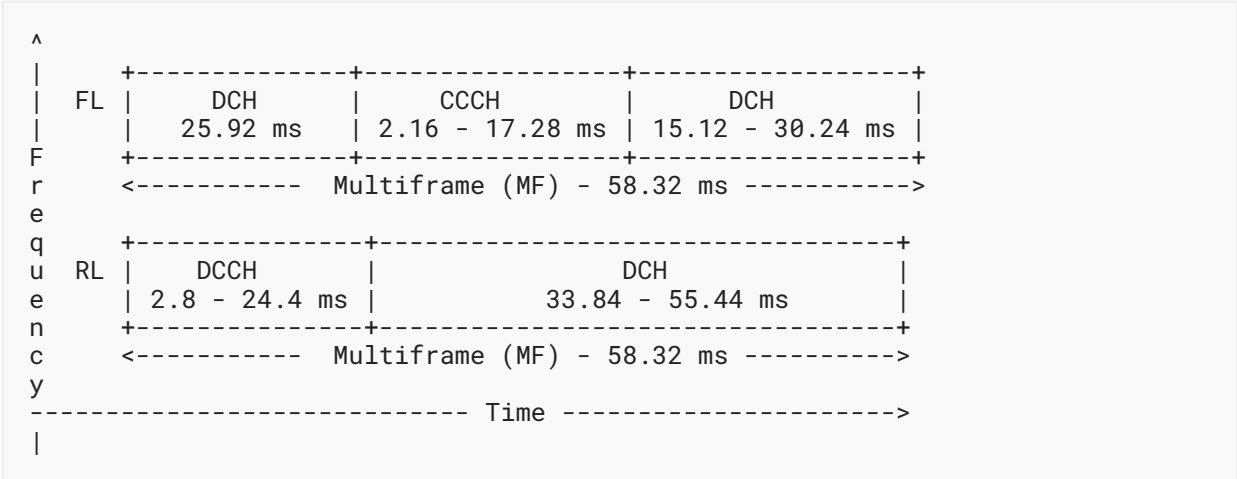


Figure 4: MF Structure for LDACS

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 QoS in LDACS medium access is to provide prioritized medium access at the bottleneck (the wireless link). Signaling of higher-layer QoS requests to LDACS is implemented on the basis of Differentiated Services (Diffserv) classes CS01 (lowest priority) to CS07 (highest priority).

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 also anchored in the LME.

In addition to radio resource management, the LDACS control channels are also used to send keepalive messages when they are not otherwise used. Since the framing of the control channels is deterministic, missing keepalive messages can be immediately detected. This information is made available to the multilink 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 (NETCONF) 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 DCH. It employs selective repeat ARQ with transparent fragmentation and reassembly to the resource allocation size to minimize latency and 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 GSs. However, there are four aspects that need to be taken into consideration: (1) scarcity of aeronautical spectrum for data link communication (tens of MHz in the L-band in the case of LDACS), (2) an increase in the number of GSs also increases the individual bandwidth for aircraft in the cell, as fewer aircraft have to share the spectrum, (3) covering worldwide terrestrial ATM via LDACS is also a question of cost and the possible reuse of spectrum, which makes it not always possible to decrease cell sizes, and (4) the Distance Measuring Equipment (DME) is the primary user of the aeronautical L-band, which means any LDACS deployment has to take DME frequency planning into account.

While aspect (2) provides a good reason alongside increasing redundancy for smaller cells than the maximum range LDACS was developed for (200 nm), the other three need to be respected when doing so. There are preliminary works on LDACS cell planning, such as [\[MOST2018\]](#), where the authors concluded that 84 LDACS cells in Europe would be sufficient to serve European air traffic for the next 20 years.

For redundancy reasons, the aeronautical community has 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 multilink 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 highly desirable, but support needs to be adapted to the specific use case.

9. Security Considerations

The goal of this section is to inform the reader about the state of security in aeronautical communications and the state security considerations applicable for all ATN/IPS traffic and to provide an overview of the LDACS link-layer security capabilities.

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 the 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 analog voice broadcast within the aeronautical VHF band. Currently, information security is mainly procedural and based by using well-trained personnel and proven communications procedures. This communication method has been in service since 1948. However, the world has changed since the emergence of civil aeronautical CNS applications in the 70s.

Civil applications have significant lower spectrum available than military applications. This means that several military defense mechanisms such as frequency hopping or pilot symbol scrambling (and thus a defense-in-depth approach starting at the physical layer) are 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 for a new type of unsophisticated listener and possible attacker.

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 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. Security in Depth

ICAO Doc 9896 [ICAO2015] foresees transport layer security for all aeronautical data transmitted via the ATN/IPS, as described in ARINC 858 [ARI2021]. This is realized via Datagram Transport Layer Security (DTLS) 1.3 [RFC9147].

LDACS also needs to comply with in-depth security requirements as stated in ARINC 858 for the radio access technologies transporting ATN/IPS data. These requirements imply that LDACS must provide Layer 2 security in addition to any higher-layer mechanisms. Specifically, ARINC 858 [ARI2021] states that data links within the FCI need to provide

a secure channel between the airborne radio systems and the peer radio access endpoints on the ground [...] to ensure authentication and integrity of air-ground message exchanges in support of an overall defense-in-depth security strategy.

9.3. LDACS Security Requirements

Overall, cybersecurity for CNS technology shall protect the following business goals [MAE20181]:

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

To further analyze assets, derive threats, and create protection scenarios, several threat and risk analyses were performed for LDACS [MAE20181] [MAE20191]. These results allowed the derivation of security scope and objectives from the requirements and the conducted threat and risk analysis. Note, IPv6 security considerations are briefly discussed in Section 9.7 while a summary of security requirements for link-layer candidates in the ATN/IPS is given in [ARI2021], which states:

Since the communication radios connect to local airborne networks in the aircraft control domain, [...] the airborne radio systems represent the first point of entry for an external threat to the aircraft. Consequently, a secure channel between the airborne radio systems and the peer radio access endpoints on the ground is necessary to ensure

authentication and integrity of air-ground message exchanges in support of an overall defense-in-depth security strategy.

9.4. LDACS Security Objectives

Security considerations for LDACS are defined by the official SARPS document by ICAO [ICAO2022]:

- LDACS shall provide a capability to protect the availability and continuity of the system.
- LDACS shall provide a capability including cryptographic mechanisms to protect the integrity of messages in transit.
- LDACS shall provide a capability to ensure the authenticity of messages in transit.
- LDACS should provide a capability for non-repudiation of origin for messages in transit.
- LDACS should provide a capability to protect the confidentiality of messages in transit.
- LDACS shall provide an authentication capability.
- LDACS shall provide a capability to authorize the permitted actions of users of the system and to deny actions that are not explicitly authorized.
- If LDACS provides interfaces to multiple domains, LDACS shall provide capability to prevent the propagation of intrusions within LDACS domains and towards external domains.

Work in 2022 includes 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.

9.5. 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].

9.6. LDACS Security Architecture

The requirements lead to an 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 [ICAO2022] and [MAE20182], and respective updates can be found in [MAE20191], [MAE20192], [MAE2020], and [MAE2021].

9.6.1. 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]; both entities provide access to the ground IPS network via an A/G LDACS router. This router is attached to an internal LDACS access network that connects via further AC-Rs to the

different LDACS cell ranges, each controlled by a GS (serving one LDACS cell), with several interconnected GSs spanning a local LDACS access network. Via the A/G wireless LDACS data link AS, the aircraft is connected to the ground network. Via the aircraft's VI and network interface, the aircraft's data can be sent via the AS back to the GS, then to the LDACS local access network, AC-Rs, LDACS access network, A/G LDACS router, and finally to the ground IPS network [ICAO2015].

9.6.2. Entity Identification

LDACS needs specific identities for the AS, the GS, and the network operator. The aircraft itself can be identified using the 24-bit ICAO identifier of an aircraft [ICAO2022], 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 LDACS AS 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 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]).

9.6.3. 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, provide proof of the ownership of their respective public key and 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 then secure all ground connections. How this process is handled in detail is still an ongoing discussion. However, established methods to secure the user plane by IPsec [RFC4301] and IKEv2 [RFC7296] or the application layer via TLS 1.3 [RFC8446] are conceivable. The LDACS PKI with its 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 [GRA2020] and (2) a 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 greater than 30 years) and the security of current pre-quantum cryptography, these security levels include pre-quantum and post-quantum cryptographic solutions. Limiting security data on the LDACS data link 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 [NIST2013], while post-quantum solutions consider Falcon [SON2021] [MAE2021] or similar lightweight PQC signature schemes and CRYSTALS-KYBER or SABER as key establishment options [AVA2021] [ROY2020].

9.6.4. 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 [ICAO2022]. This possibility of providing low-layered confidentiality and integrity protection ensures a secure delivery of user data over the wireless link. Furthermore, it ensures integrity protection of LDACS control data.

9.7. Considerations on LDACS Security Impact on IPv6 Operational Security

In this part, considerations on IPv6 operational security in [RFC9099] and interrelations with the LDACS security additions are compared and evaluated to identify further protection demands. As IPv6 heavily relies on the Neighbor Discovery Protocol (NDP) [RFC4861], integrity and authenticity protection on the link layer, as provided by LDACS, already help mitigate spoofing and redirection attacks. However, to also mitigate the threat of remote DDoS attacks, neighbor solicitation rate-limiting is recommended by [RFC9099]. To prevent the threat of DDoS and DoS attacks in general on the LDACS access network, rate-limiting needs to be performed on each network node in the LDACS access network. One approach is to filter for the total amount of possible LDACS AS-GS traffic per cell (i.e., of up to 1.4 Mbit/s user data per cell and up to the amount of GS per service provider network times 1.4 Mbit/s).

10. IANA Considerations

This document has no IANA actions.

11. Informative References

- [ARI2019] ARINC, "AOC AIR-GROUND DATA AND MESSAGE EXCHANGE FORMAT", ARINC 633, January 2019, <<https://standards.globalspec.com/std/13152055/ARINC%20633>>.
- [ARI2020] "Aeronautical Radio Incorporated (ARINC) Industry Activities", <<https://www.aviation-ia.com/>>.
- [ARI2021] ARINC, "INTERNET PROTOCOL SUITE (IPS) FOR AERONAUTICAL SAFETY SERVICES PART 1 AIRBORNE IPS SYSTEM TECHNICAL REQUIREMENTS", ARINC 858P1, June 2021, <<https://standards.globalspec.com/std/14391274/858p1>>.
- [AVA2021] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., and D. Stehlé, "CRYSTALS-KYBER - Algorithm Specification and Supporting Documentation (version 3.02)", August 2021, <<https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf>>.

- [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, DOI 10.1109/DASC43569.2019.9081678, September 2019, <<https://doi.org/10.1109/DASC43569.2019.9081678>>.
- [BEL2021]** Bellido-Manganell, M.A., Gräupl, T., Heirich, O., Mäurer, 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, Vol. 58, Issue 1, pp. 615-634, DOI 10.1109/TAES.2021.3111722, September 2021, <<https://doi.org/10.1109/TAES.2021.3111722>>.
- [BIL2017]** Bilzhause, A., Belgacem, B., Mostafa, M., and T. Gräupl, "Datalink security in the L-band digital aeronautical communications system (LDACS) for air traffic management", IEEE Aerospace and Electronic Systems Magazine, Vol. 32, Issue 11, pp. 22-33, DOI 10.1109/MAES.2017.160282, November 2017, <<https://doi.org/10.1109/MAES.2017.160282>>.
- [BOE2019]** Boegl, T., Rautenberg, M., Haindl, R., Rihacek, C., Meser, J., Fantappie, P., Pringvanich, N., Micallef, J., Hauf, K., MacBride, J., Sacre, P., v.d. Eiden, B., Gräupl, 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, October 2019.
- [CRO2016]** Crowe, B., "Proposed AeroMACS PKI specification is a model for global and National Aeronautical PKI Deployments", Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-19, DOI 10.1109/ICNSURV.2016.7486405, April 2016, <<https://doi.org/10.1109/ICNSURV.2016.7486405>>.
- [DO350A]** RTCA, "Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)", Vol. 1 & 2, RTCA DO-350, March 2016, <<https://standards.globalspec.com/std/10003192/rtca-do-350-volume-1-2>>.
- [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/>>.
- [FAA2020]** Federal Aviation Administration, "ADS-B Privacy", February 2023, <https://www.faa.gov/air_traffic/technology/equipadsb/privacy>.
- [GNU2021]** GNU Radio Project, "GNU Radio", <<http://gnuradio.org>>.
- [GRA2011]** Gräupl, T. and M. Ehammer, "LDACS1 data link layer evolution for ATN/IPS", IEEE/AIAA 30th Digital Avionics Systems Conference (DASC), pp. 1-28, DOI 10.1109/DASC.2011.6096230, October 2011, <<https://doi.org/10.1109/DASC.2011.6096230>>.

- [GRA2018]** Gräupl, T., Schneckenburger, N., Jost, T., Schnell, M., Filip, A., Bellido-Manganell, M.A., Mielke, D.M., Mäurer, 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, DOI 10.1109/ICNSURV.2018.8384881, April 2018, <<https://doi.org/10.1109/ICNSURV.2018.8384881>>.
- [GRA2020]** Gräupl, T., "Initial LDACS A/G Specification", SESAR2020 - PJ14-W2-60, D3.1.210, December 2020, <https://www.ldacs.com/wp-content/uploads/2013/12/SESAR2020_PJ14-W2-60_D3_1_210_Initial_LDACS_AG_Specification_00_01_00-1_0_updated.pdf>.
- [ICAO2015]** International Civil Aviation Organization (ICAO), "Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocol", ICAO 9896, January 2015, <<https://standards.globalspec.com/std/10026940/icao-9896>>.
- [ICAO2018]** International Civil Aviation Organization (ICAO), "Handbook on Radio Frequency Spectrum Requirements for Civil Aviation", Vol. 1, ICAO Spectrum Strategy, Policy Statements and Related Information, Doc 9718, AN/957, July 2018, <[https://www.icao.int/safety/FSMP/Documents/Doc9718/Doc.9718%20Vol.%20I%20\(AdvanceUneditedVersion%202021\).pdf](https://www.icao.int/safety/FSMP/Documents/Doc9718/Doc.9718%20Vol.%20I%20(AdvanceUneditedVersion%202021).pdf)>.
- [ICAO2019]** International Civil Aviation Organization (ICAO), "Manual on VHF Digital Link (VDL) Mode 2", Second Edition, Doc 9776, 2015, <<https://store.icao.int/en/manual-on-vhf-digital-link-vdl-mode-2-doc-9776>>.
- [ICAO2022]** International Civil Aviation Organization (ICAO), "CHAPTER 13 L-Band Digital Aeronautical Communications System (LDACS)", International Standards and Recommended Practices, Annex 10 - Aeronautical Telecommunications, Volume III, Communication Systems, 2022, <https://www.ldacs.com/wp-content/uploads/2023/03/WP06.AppA-DCIWG-6-LDACS_SARPs.pdf>.
- [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, DOI 10.1109/ICNSURV.2010.5503256, May 2010, <<https://doi.org/10.1109/ICNSURV.2010.5503256>>.
- [KAMA2018]** Kamali, B., "AeroMACS: An IEEE 802.16 Standard-Based Technology for the Next Generation of Air Transportation Systems", DOI 10.1002/9781119281139, September 2018, <<https://doi.org/10.1002/9781119281139>>.
- [LISP-GB-ATN]** Haindl, B., Lindner, M., Moreno, V., Portoles-Comeras, M., Maino, F., and B. Venkatachalapathy, "Ground-Based LISP for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-haindl-lisp-gb-atn-08, 23 September 2022, <<https://datatracker.ietf.org/doc/html/draft-haindl-lisp-gb-atn-08>>.

- [MAE20181]** Mäurer, 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, DOI 10.1109/ICNSURV.2018.8384828, April 2018, <<https://doi.org/10.1109/ICNSURV.2018.8384828>>.
- [MAE20182]** Mäurer, N. and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)", IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), pp. 1-10, DOI 10.1109/DASC.2018.8569878, September 2018, <<https://doi.org/10.1109/DASC.2018.8569878>>.
- [MAE20191]** Mäurer, N., Gräupl, T., and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation", IEEE 38th Digital Avionics Systems Conference (DASC), pp. 1-10, DOI 10.1109/DASC43569.2019.9081786, September 2019, <<https://doi.org/10.1109/DASC43569.2019.9081786>>.
- [MAE20192]** Mäurer, 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, DOI 10.1109/ICNSURV.2019.8735139, April 2019, <<https://doi.org/10.1109/ICNSURV.2019.8735139>>.
- [MAE2020]** Mäurer, N., Gräupl, T., Gentsch, C., and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS", IEEE/AIAA 39th Digital Avionics Systems Conference (DASC), pp. 1-10, DOI 10.1109/DASC50938.2020.9256746, October 2020, <<https://doi.org/10.1109/DASC50938.2020.9256746>>.
- [MAE2021]** Mäurer, N., Gräupl, T., Gentsch, C., Guggemos, T., Tiepelt, M., Schmitt, C., and G. Dreo Rodosek, "A Secure Cell-Attachment Procedure for LDACS", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 1-10, DOI 10.1109/EuroSPW54576.2021.00019, September 2021, <<https://doi.org/10.1109/EuroSPW54576.2021.00019>>.
- [MAE20211]** Mäurer, N., Gräupl, T., Bellido-Manganell, M.A., Mielke, D.M., Filip-Dhaubhadel, A., Heirich, O., Gerberth, D., Felux, 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, Vol. 36, Issue 4, pp. 8-17, DOI 10.1109/MAES.2021.3052318, April 2021, <<https://doi.org/10.1109/MAES.2021.3052318>>.
- [MOST2018]** Mostafa, M., Bellido-Manganell, M.A., and T. Gräupl, "Feasibility of Cell Planning for the L-Band Digital Aeronautical Communications System Under the Constraint of Secondary Spectrum Usage", IEEE Transactions on Vehicular Technology, Vol. 67, Issue 10, pp. 9721-9733, DOI 10.1109/TVT.2018.2862829, October 2018, <<https://doi.org/10.1109/TVT.2018.2862829>>.

- [NIST2013]** National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", FIPS PUB 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013, <<https://doi.org/10.6028/NIST.FIPS.186-4>>.
- [OSE2019]** Osechas, O., Narayanan, S., Crespillo, O.G., Zampieri, G., Battista, G., Kumar, R., Schneckenburger, N., Lay, E., Belabbas, B., and M. Meurer, "Feasibility Demonstration of Terrestrial RNP with LDACS", 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation, pp. 3254-3265, DOI 10.33012/2019.17119, September 2019, <<https://doi.org/10.33012/2019.17119>>.
- [RAW-TECHNOS]** Thubert, P., Ed., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-ietf-raw-technologies-06, 30 November 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-raw-technologies-06>>.
- [RAW-USE-CASES]** Bernardos, C. J., Ed., Papadopoulos, G. Z., Thubert, P., and F. Theoleyre, "RAW Use-Cases", Work in Progress, Internet-Draft, draft-ietf-raw-use-cases-09, 13 March 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-raw-use-cases-08>>.
- [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>>.
- [RFC4861]** Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC5213]** Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<https://www.rfc-editor.org/info/rfc5213>>.
- [RFC5795]** Sandlund, K., Pelletier, G., and L. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, DOI 10.17487/RFC5795, March 2010, <<https://www.rfc-editor.org/info/rfc5795>>.
- [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>>.
- [RFC8200]** Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [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>>.

-
- [RFC9099] Vyncke, É., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <<https://www.rfc-editor.org/info/rfc9099>>.
- [RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <<https://www.rfc-editor.org/info/rfc9147>>.
- [RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <<https://www.rfc-editor.org/info/rfc9300>>.
- [RFC9301] Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", RFC 9301, DOI 10.17487/RFC9301, October 2022, <<https://www.rfc-editor.org/info/rfc9301>>.
- [RIH2018] Rihacek, C., Haindl, B., Fantappie, P., Pierattelli, S., Gräupl, 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, DOI 10.1109/ICNSURV.2018.8384880, April 2018, <<https://doi.org/10.1109/ICNSURV.2018.8384880>>.
- [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, Vol. 2020, Issue 4, pp. 443-466, DOI 10.13154/tches.v2020.i4.443-466, August 2020, <<https://doi.org/10.13154/tches.v2020.i4.443-466>>.
- [RTCA2019] Radio Technical Commission for Aeronautics (RTCA), "Internet Protocol Suite Profiles", RTCA DO-379, September 2019, <<https://standards.globalspec.com/std/14224450/rtca-do-379>>.
- [RTGWG-ATN-BGP] Templin, F., Ed., 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-19, 7 November 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-rtgwg-atn-bgp-19>>.
- [SAJ2014] Haindl, B., Meser, J., Sajatovic, M., Müller, S., Arthaber, H., Faseth, T., and M. Zaisberger, "LDACS1 conformance and compatibility assessment", IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), pp. 1-11, DOI 10.1109/DASC.2014.6979447, October 2014, <<https://doi.org/10.1109/DASC.2014.6979447>>.
- [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, Vol. 52, Issue 5, pp. 2281-2297, DOI 10.1109/TAES.2016.150451, October 2016, <<https://doi.org/10.1109/TAES.2016.150451>>.
-

- [SCHN2018] Schneckenburger, N., "A Wide-Band Air-Ground Channel Model", Dissertation, Technischen Universitaet Ilmenau, February 2018.
- [SHU2013] Shutin, D., Schneckenburger, N., Walter, M., and M. Schnell, "LDACS1 ranging performance - An analysis of flight measurement results", IEEE 32nd Digital Avionics Systems Conference (DASC), pp. 1-10, DOI 10.1109/DASC.2013.6712567, October 2013, <<https://doi.org/10.1109/DASC.2013.6712567>>.
- [SIT2020] "Societe Internationale de Telecommunica Aéronautique (SITA)", <<https://www.sita.aero/>>.
- [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, DOI 10.1007/978-3-030-57682-0_3, 2021, <https://doi.org/10.1007/978-3-030-57682-0_3>.
- [STR2016] Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., and I. Martinovic, "On Perception and Reality in Wireless Air Traffic Communication Security", IEEE Transactions on Intelligent Transportation Systems, Vol. 18, Issue 6, pp. 1338-1357, DOI 10.1109/TITS.2016.2612584, October 2016, <<https://doi.org/10.1109/TITS.2016.2612584>>.
- [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, Vol. 22, Issue 8, pp. 4864-4875, DOI 10.1109/TITS.2020.2983614, August 2021, <<https://doi.org/10.1109/TITS.2020.2983614>>.

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 Communications
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	0.989	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 to 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	0.989	0.989	0.989

	RSP 160	RSP 160	RSP 180	RSP 180	RSP 400	RSP 400
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 to 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.

Acknowledgements

Thanks to all contributors to the development of LDACS and ICAO Project Team Terrestrial (PT-T), as well as to all in the RAW Working Group for deep discussions and feedback.

Thanks to Klaus-Peter Hauf, Bart Van Den Einden, and Pierluigi Fantappie for their comments on this document.

Thanks to the Chair of Network Security for input and to the Research Institute CODE for their comments and improvements.

Thanks to the colleagues of the Research Institute CODE at the UniBwM, who are working on the AMIUS project funded under the Bavarian Aerospace Program by the Bavarian State Ministry of Economics, Regional Development and Energy with the GA ROB-2-3410.20-04-11-15/HAMI-2109-0015, for fruitful discussions on aeronautical communications and relevant security incentives for the target market.

Thanks to SBA Research Vienna for continuous discussions on security infrastructure issues in quickly developing markets such as the air space and potential economic spillovers to used technologies and protocols.

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.

Authors' Addresses

Nils Mäurer (EDITOR)

German Aerospace Center (DLR)
Münchner Strasse 20
82234 Wessling
Germany
Email: Nils.Maeurer@dlr.de

Thomas Gräupl (EDITOR)

German Aerospace Center (DLR)
Münchner Strasse 20
82234 Wessling
Germany
Email: Thomas.Graeupl@dlr.de

Corinna Schmitt (EDITOR)

Research Institute CODE, UniBwM
Werner-Heisenberg-Weg 39
85577 Neubiberg
Germany
Email: corinna.schmitt@unibw.de