# L-band Digital Aeronautical Communications System (LDACS)

draft-ietf-raw-ldacs-05

Nils Mäurer, Thomas Gräupl, Corinna Schmitt

# Note Well

**This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.**

**As a reminder:**

- **By participating in the IETF, you agree to follow IETF processes and policies.**
- **If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.**
- **As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.**
- **Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.**
- **As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam ( https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.**

**Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:**

**BCP 9 (Internet Standards Process)**

**BCP 25 (Working Group processes)**

**BCP 25 (Anti-Harassment Procedures)**

**BCP 54 (Code of Conduct)**

**BCP 78 (Copyright)**


**BCP 79 (Patents, Participation)**

**https://www.ietf.org/privacy-policy/ (Privacy Policy)**

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

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

1 November 2020

# L-band Digital Aeronautical Communications System (LDACS)
draft-ietf-raw-ldacs-05

Abstract

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

## draft-meaurer-raw-04 (IETF 108)

Table of Contents


1. Introduction . . . . . 3
2. Terminology . . . . . 3
3. Motivation and Use Cases . . . . . 4
3.1. Voice Communications Today . . . . . 5
3.2. Data Communications Today . . . . . 5
4. Provenance and Documents . . . . . 6
5. Applicability . . . . . 7
5.1. Advances Beyond the State-of-the-Art . . . . . 7
5.1.1. Priorities . . . . . 7
5.1.2. Security . . . . . 8
5.1.3. High Data Rates . . . . . 8
5.2. Application . . . . . 8
5.2.1. Air-to-Ground Multilink . . . . . 8
5.2.2. Air-to-Air Extension for LDACS . . . . . 9
5.2.3. Flight Guidance . . . . . 9
5.2.4. Business Communication of Airlines . . . . . 10
5.2.5. LDACS Navigation . . . . . 10
6. Characteristics of LDACS . . . . . 11
6.1. LDACS Sub-Network . . . . . 11
6.2. Topology . . . . . 12
6.3. LDACS Physical Layer . . . . . 12
6.4. LDACS Data Link Layer . . . . . 12
6.5. LDACS Mobility . . . . . 13
7. Reliability and Availability . . . . . 13
8. Protocol Stack . . . . . 15
8.1. Medium Access Control (MAC) Entity Services . . . . . 16
8.2. Data Link Service (DLS) Entity Services . . . . . 18
8.3. Voice Interface (VI) Services . . . . . 19
8.4. LDACS Management Entity (LME) Services . . . . . 19
8.5. Sub-Network Protocol (SNP) Services . . . . . 19
9. Security Considerations . . . . . 19
10. Privacy Considerations . . . . . 20
11. IANA Considerations . . . . . 20
12. Acknowledgements . . . . . 20
13. Normative References . . . . . 21
14. Informative References . . . . . 21
Authors' Addresses . . . . . 23


Changes

## draft-ietf-raw-05 (IETF 109)

Table of Contents


1. Introduction . . . . . 3
1.1. Requirements Language . . . . . 4
2. Terminology . . . . . 4
3. Motivation and Use Cases . . . . . 5
3.1. Voice Communications Today . . . . . 5
3.2. Data Communications Today . . . . . 6
4. Provenance and Documents . . . . . 7
5. Applicability . . . . . 8
5.1. Advances Beyond the State-of-the-Art . . . . . 8
5.1.1. Priorities . . . . . 8
5.1.2. Security . . . . . 8
5.1.3. High Data Rates . . . . . 9
5.2. Application . . . . . 9
5.2.1. Air-to-Ground Multilink . . . . . 9
5.2.2. Air-to-Air Extension for LDACS . . . . . 9
5.2.3. Flight Guidance . . . . . 10
5.2.4. Business Communication of Airlines . . . . . 11
5.2.5. LDACS Navigation . . . . . 11
6. Requirements to LDACS . . . . . 11
7. Characteristics of LDACS . . . . . 13
7.1. LDACS Sub-Network . . . . . 13
7.2. Topology . . . . . 14
7.3. LDACS Physical Layer . . . . . 14
7.4. LDACS Data Link Layer . . . . . 15
7.5. LDACS Mobility . . . . . 15
8. Reliability and Availability . . . . . 15
8.1. Layer 2 . . . . . 15
8.2. Beyond Layer 2 . . . . . 18
9. Protocol Stack . . . . . 18
9.1. MAC Entity Services . . . . . 19
9.2. DLS Entity Services . . . . . 21
9.3. VI Services . . . . . 22
9.4. LME Services . . . . . 22
9.5. SNP Services . . . . . 22
10. Security Considerations . . . . . 22
10.1. Reasons for Wireless Digital Aeronautical Communications . . . . . 22
10.2. Requirements for LDACS . . . . . 23
10.3. Security Objectives for LDACS . . . . . 24
10.4. Security Functions for LDACS . . . . . 24
10.5. Security Architectural Details for LDACS . . . . . 24
10.5.1. Entities in LDACS Security Model . . . . . 25
10.5.2. Matter of LDACS Entity Identification . . . . . 25
10.5.3. Matter of LDACS Entity Authentication and Key Negotiation . . . . . 25
10.5.4. Matter of LDACS Message-in-transit Confidentiality, Integrity and Authenticity . . . . . 26
10.6. Security Architecture for LDACS . . . . . 26
11. Privacy Considerations . . . . . 27
12. IANA Considerations . . . . . 27
13. Acknowledgements . . . . . 27
14. Normative References . . . . . 27
15. Informative References . . . . . 27
Appendix A. Selected Information from DO-350A . . . . . 30
Authors' Addresses . . . . . 32

# Chapter 6 – Requirements to LDACS (1)

- Application area: Communication related to flight safety & regularity

- Challenges:
  - Heavy regulation worldwide and spectrum scarcity
  - Data links **MAY** only use aviation licensed spectrum
  - Not enough bandwidth on terrestrical data links

- Idea/Plan:
  - Use of non-aviation specific data links → security issues exist
  - Aeronautical IP internetwork & Internet **SHOULD** be separated completely

# Chapter 6 – Requirements to LDACS (2)

- Objective of LDACS:
  - **Replace** legacy OSI stack and proprietary ACARS with industry standard IP technology
  - **Provide** a next generation terrestrial data link designed to support IP and provide much higher bandwidth

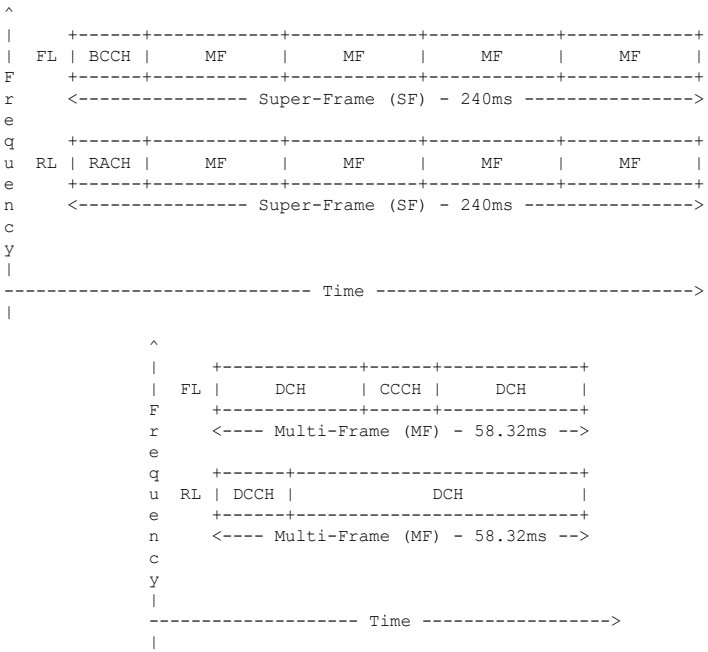
- Requirement for LDACS:
  - **Provide** a terrestrial high-throughput data link for IP internetworking in the aircraft
  - **Interoperability** with IP at the gateway connecting the LDACS network to other aeronautical ground networks is a **MUST**

# Chapter 8 – Reliability & Availability (1)

- PHY layer:
  - OFDM-based Frequency Division Duplex system
  - Deployed in aeronautical communications restrcted L-band with 500kHz bandwidth
  - Guard times allow operations in up to 200 NM range
  - LDACS FL physical layer is a continuous OFDM transmission
  - LDACS RL transmission is based on OFDMA-TDMA bursts
  - User data: Adaptive coding and modulation
  - Control data: most robust coding and modulation

# Chapter 8 – Reliability & Availability (2)

- MAC layer:
  - Static frame structure to support deterministic timer management
  - MAC: Always managed by Ground Station (GS)
  - GS: Handles resource management (Resource requests and allocation)
  - Resource requests: On demand or permanent
  - User data transmissions over LDACS always scheduled by GS
  - Control data uses statically (i.e. at cell entry) allocated recurring resources
  - GS handles cell load (e.g. can force handovers)



# Chapter 8 – Reliability & Availability (3)

- DLL layer:
  - ARQ providing reliable data transmission on layer 2
  - Selective repeat ARQ with transparent fragmentation and reassembly to the resource allocation size
  - Achieving low latency and low overhead without losing reliability
  - Ensuring correct order of packet delivery without duplicates
  - Identifies lost fragments with deterministic timers synced to the medium access frame structure and initiates retransmission
  - Priority mechanism of LDACS ensures the timely delivery of messages with high importance

# Chapter 10 – Security Considerations (1)

- Problem: Changed Threat-Landscape

- Consequences:
  - Future digital communications waveforms require embedded security features
  - Security features require sufficient bandwidth (beyond the capabilities of VHF narrowband communications system)
  - With progress of digitalization (automated procedures such as 4D-Trajectories allowing semi-automated en-route flying of aircraft)

- Strong cybersecurity measures are a **MUST** for LDACS

# Chapter 10 – Security Considerations (2)

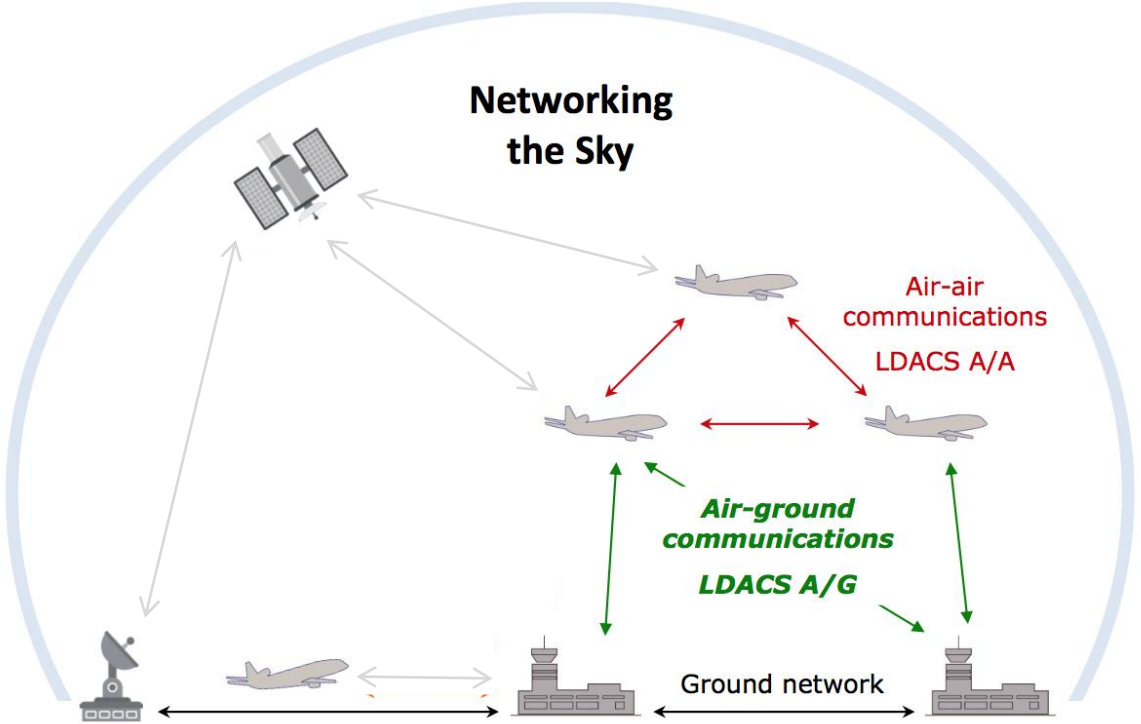
- LDACS's Security:
  - **SHALL** protect availability & continuity
  - **SHALL** protect the integrity of messages in transit
  - **SHALL** provide authenticity of messages in transit
  - **SHOULD** provide confidentiality of messages in transit
  - **SHOULD** provide non-repudiation for necessary messages in transit
  - **SHALL** provide mutual authentication
  - **SHALL** authorize the permitted actions of users & deny actions else
  - **SHALL** provide capability preventing the propagation of intrusions within LDACS domains & towards external domains

# Chapter 10 – Security Considerations (3)

- Resulting Security Architectural Details (Section 10.5):
  - Entities in LDACS Security Mode
  - Matter of
    - Trust in LDACS System
    - Entity Identification
    - Entity Authentication and Key Negotiation
    - Message-in-transit Confidentiality, Integrity and Authenticity

- Security Moduls (Section 10.6):
  - PKI with public key certificates incorporated in the PKI based chain-of-trust
  - Identity management based on aircraft identities & network operator identities
  - Certificates stored in the entities allowing
  - Mutual authentication & key exchange procedures
  - Key derivation mechanisms for perfect forward secrecy
  - User/control plane message-in-transit integrity & confidentiality protection

# Thanks


Networking
the Sky
Air-air
communications
LDACS A/A
Air-ground
communications
LDACS A/G
Ground network