Evaluation of the LDACS Cybersecurity Implementation

Nils Mäurer and Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{nils.maeurer, thomas.graeupl}@dlr.de

Corinna Schmitt
Research Institute CODE
Bundeswehr University Munich
Munich, Germany
corinna.schmitt@unibw.de

***Abstract*—Communication, Navigation and Surveillance (CNS) infrastructure in civil aviation must evolve as fast as possible to cope with all challenges posed by the growth of the worldwide population, globalization and the demand for more and more mobility worldwide. Analogue systems are replaced by digital means, automation is becoming much more important to handle new entrants in the air traffic system, spectrum saturation must be solved by introducing digital systems and the safety and security of the safety critical infrastructure surrounding civil aviation must be constantly updated to support the ever-growing complexity of the system. As one of the Future Communication Infrastructure (FCI) candidates we introduce LDACS as the very first true integrated CNS system worldwide. In previous works we have already analyzed its cybersecurity and developed an architecture with corresponding algorithm and proofed the improvement of the cybersecurity due to our security additions. Here we implement the LDACS cybersecurity architecture and evaluate the impact of introduced security overhead on the LDACS system. We conclude that the proposed protection mechanisms successfully mitigate previously identified risks and only add minor time, data and computation overhead on top of the LDACS protocol stack, making the security solutions a good candidate to be included in the SESAR wave 2 updated LDACS specification.**

***Index Terms*—LDACS, Cybersecurity, FCI, Digital Datalink, Security Architecture**

I. Introduction

In its latest Challenges of Growth study EUROCONTROL estimates that civil air traffic will grow by a significant rate of 84% until 2040. Under this estimation it is expected that legacy Air Traffic Management (ATM) systems will surpass their capacity limits [8].

Saturation of the VHF band, spectrum depletion, new entrants such as drones in the air space, new technologies enabling automatized transportation of goods or people and with the growth of the entire population and thus an increased need for transportation are challenges that must be solved to cope with the growth [8], [31], [33]. One answer to enable quicker, faster and safer handling of air traffic participants is to successfully conduct the transition from analogue to digital communication in worldwide ATM for Communication Navigation and Surveillance (CNS) systems [32].

With the Single European Sky ATM Research (SESAR) program of the EU and its counterpart NextGEN in the US, several new digital aeronautical communication technologies are currently under development [8], [33]. The main goal of both is to develop enabling technologies to cope with the expected air traffic growth. These technologies shall make more efficient use of the limited aeronautical spectrum by transitioning from analogue voice to digital data communication [32]. Candidates for the Future Aeronautical Communication Infrastructure (FCI) are AeroMACS for airport communications, SatCOM for remote domains, and LDACS (L-band Digital Aeronautical Communications System) for long-range terrestrial aeronautical communications system. Figure 1 illustrates where these candidates are envisioned to be located. LDACS is developed in Europe and currently under standardization by the International Civil Aviation Organization (ICAO). LDACS, as terrestrial digital wireless communication system, enables communication, navigation and surveillance at the same time and by that it is the world's first true integrated CNS system [26]. The communication capabilities of LDACS consist of two parts: (1) the Air-Ground link for long-range terrestrial communication and (2) a link for Air-Air communications currently developed by DLR.

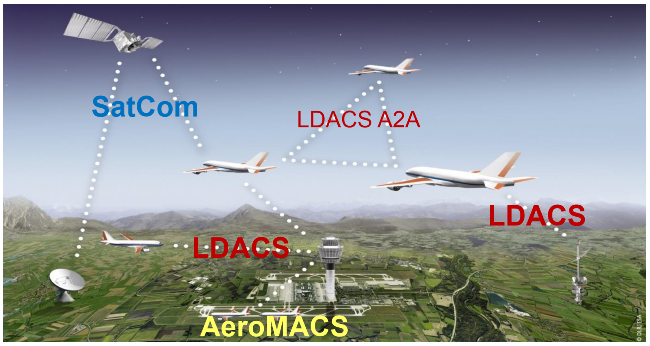


Fig. 1. Future Communications Infrastructure (FCI) [26]

In this paper we focus on the Air-Ground link. It ensures safety and regularity of flight and is based on technologies used in the 3G and 4G mobile phone network [29]. It has been adapted for safety critical infrastructure requirements and shall be deployed as an inlay system in the L-band next to the Distance Measurement Equipment (DME) as illustrated in Figure 3 [1], [25]. With the augmentation of

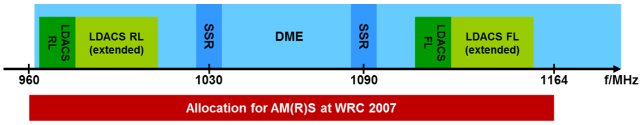


Fig. 2. Frequency assignment for LDACS at WRC 2007, next to DME

analogue systems by digital substitutes and the related trend towards an increased autonomous data processing as justified in [32], LDACS requires a thorough cybersecurity analysis and cybersecurity architectural design [20]. The envisioned analysis and design should be similar to the ones used in 3G, 4G, or AeroMACS [5], [11].

In [1], [19], [20] a preliminary draft of a a cybersecurity architecture for LDACS was justified and presented. In these references it was clearly stated that essential requirements were imposed by the aeronautical spectrum environment (e.g., reduced spectrum bandwidth and limited data rates). In order to develop a successful cybersecurity solution for LDACS, existing security protocols and algorithms had to be analyzed in terms of resource consumption and compatibility. Thus, this paper presents a comparison of investigated security protocol implementations for LDACS. Further, simulations were done in order to estimate the additional overhead security brings to the current LDACS protocol. Initial results during flight trials show that overhead is negligible compared to the security improvement in the protocol itself.

This paper is structured as follows: Section II presents basic knowledge of LDACS before the new LDACS's cybersecurity architecture is introduced in Section III. Implementation details with focus on software simulations of LDACS are presented in Section IV. The gained results are explained in Section V before concluding the paper in Section VI.

II. Background on LDACS

The L-band Digital Aeronautical Communications System (LDACS) is the terrestrial data link in the Future Communications Infrastructure (FCI). In 2007 the Federal Aviation Administration (FAA) and EUROCONTROL started a joint investigation on existing technologies to investigate if any technology could fulfill the demands of growing ATM in the future. In short, the answer was no and, thus, sparked the development of LDACS [7].

A. System Characteristics

The realized LDACS has its origin in merging parts of the B-VHF [3], B-AMC [24], [27], TIA-902 (P34) [16], and WiMAX IEEE 802.16e technologies [6]. In 2007 the spectrum for LDACS was allocated at the World Radio Conference (WRC). It was decided to allocate the spectrum next to DME, resulting in an inlay approach between the DME channels for LDACS as illustrated in Figure 3. Furthermore, LDACS uses LTE/4G-like technology (e.g., Orthogonal Frequency-Division Multiplexing) (OFDM) to remain highly flexible and scalable and efficient in coding, supporting adaptive coding and modulation. Additionally, it applies (Frequency Division Duplexing (FDD), because of the limited bandwidth available with the inlay approach and a cellular communications concept (cf. Figure 4, where each LDACS Station consists of GSC & GS). Besides all these, LDACS supports seamless handovers, data and voice transmissions, Quality-of-Service (QoS), has a navigation and surveillance extension and an air-to-air link is currently being developed. Most of those points will be clarified in the next subsections. Due to the allocation next to DME, LDACS will be deployed using an inlay approach between the DME channels.

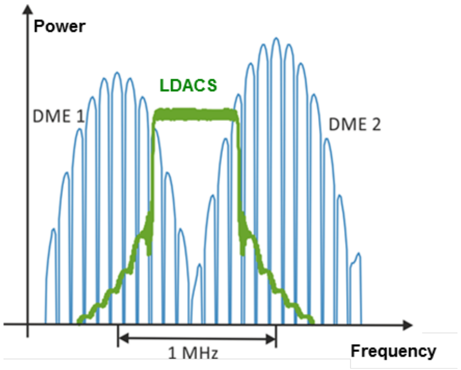


Fig. 3. Inlay approach for LDACS in between the DME bursts

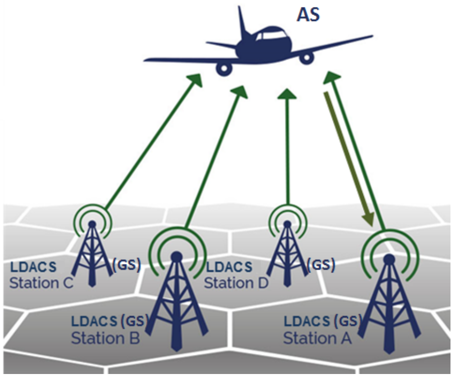


Fig. 4. Cell planning for LDACS

B. Communication Functionality

LDACS was especially designed for Air Traffic Control (ATC) and ATM applications like Controller Pilot Data Link Communications (CPDLC), Automatic Dependent Surveillance - Contract (ADS-C), full 4D trajectories exchange and real-time weather information. It is envisioned that Ground Based Augmentation System (GBAS) functionality will be provided via LDACS in the future as well. The underlying enabler for all those applications are the main LDACS parameters listed in Table I. Thus, LDACS covers current Aeronautical Operational Control (AOC) and also future applications, enables new concepts (e.g., sectorless ATM) and has at least 50 times more net capacity than VHF Data Link (VDL) Mode 2. [9]

TABLE I
MAIN PARAMETERS FOR LDACS

Number of sub carriers	64 (50 used)
Bandwidth	625 / 488 kHz
Subcarrier spacing	9.765625 kHz
OFDM symbol duration	102.4 μ
Guard interval	(4.8 + 12.8) μ
Net data rate	550 kbits - 2.6 Mbit/s

C. Entities

Aircraft Station (AS), Ground Station (GS) and Ground Station Controller (GSC) form the basic LDACS network. As mentioned in 512 aircraft can be served by one GS where the GS sends a continuous data stream in the Forward Link (FL) to the AS. The Reverse Link (RL) consists of individual bursts of data from each AS to GS. This means, for every RL communication the AS first needs to request the respective resource allocation within its cell from the GS before being able to send. Both FL and RL communication, including user and control data, is done via the air gap over the radio link between AS and GS. On the ground a GSC is responsible for serving several GSs, forming an LDACS sub-network with its LDACS internal ground network infrastructure. The GSC is linked to the LDACS access network, which in turn is linked to the Air/Ground LDACS router, being now the direct connection to the ground network. The aeronautical ground network (previously the Aeronautical Telecommunications Network (ATN)) is used for example by Air traffic Network Services Providers (ANSP) and airlines to exchange AIR Traffic Service (ATS) or Airline Operational Control (AOC) data between the ground infrastructure and the aircraft.

D. Protocol Stack

Figure 5 shows the protocol stack of LDACS as implemented in the AS and GS. It consists of the Physical Layer (PHY), the Medium Access Layer (MAC), Voice Interface (VI), Data Link Service (DLS) layer, LDACS Management Entity (LME) and Sub-Network Protocol (SNP) layer. For more details see Section III. The LDACS protocol stack is located on Layer 1, 2 and 3 of the ISO/OSI model with TCP/IP and IPv6 placed above the SNP. Below the SNP, data is fragmented, prioritized and aggregated at the DLS layer. [25] In order to communicate, LDACS uses several logical channels in the MAC layer [25]:

- The GS announces its existence and several necessary physical parameters in the Broadcast Channel (BCCH) to incoming AS.
- The Random Access Channel (RACH) enables the AS to request access to an LDACS cell.
- In the Forward Link (FL) the Common Control Channel (CCCH) is used by the GS to distribute and grant access to system resources.
- The reverse direction is covered by the Reverse Link (RL), where aircraft need to request resources (in so called resource allocation) in order to be allowed to send. This happens via the Dedicated Common Control Channel (DCCH).
- User data itself is communicated in the Data Channel (DCH) on the FL and RL.

E. Extension Towards Navigation and Surveillance

Around 2011 the development of an extension towards navigation in the sense of ”Alternative Positioning Navigation and Time” (APNT) started [28]. The concept was proven in theory in 2012 with simulations in 2013 showing achievable accuracy of the aircraft position of around 4m [22]. Later in 2013 and 2015, flight trials confirmed the localization accuracy of around 15m with demonstration equipment, while in 2019 it was set out in the German national project MICONAV [15] to test real-time positioning. All of the aforementioned steps confirm, that LDACS can be used as a true navigation substitute for En-Route (ENR) continental flights in case of DME or GPS outage. In the long term, it must be considered whether LDACS can truly replace legacy DME systems in the long-term. There are also considerations to use LDACS for surveillance such as Filip et al. showed in [10] using LDACS as a passive radar substitute. However, the easier approach to implement surveillance into LDACS is to use ADS-C and Automatic Dependent Surveillance - Broadcast (ADS-B) and broadcast the position of an aircraft to all neighboring planes and periodically send the position of that aircraft via the RL down to the ground network. As demonstrated in flight trials, LDACS can provide the three vital components for civil air traffic, being communications, navigation and surveillance, and is thus the world’s first true integrated CNS system [26].

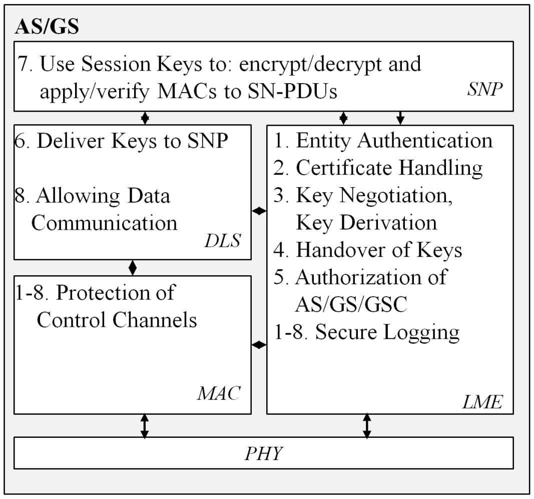


Fig. 5. Protocol Stack of LDACS

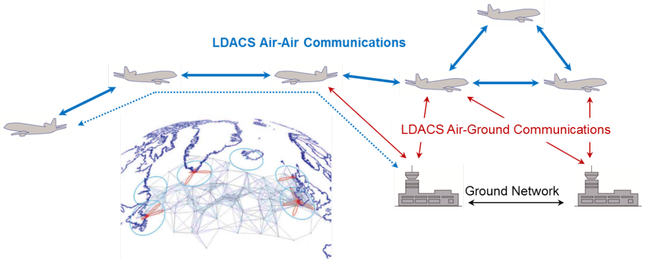


Fig. 6. Future extension of the LDACS A/G link by Air-Air (A/A) support, enabling digital aeronautical communications without ground infrastructure

F. Extension Towards Aircraft Connectivity

The latest extension of LDACS – the Air-Air communication – covered in the German national project IntAirNet [26]. The goal was to establish direct Air-Air communications between aircraft in communication range allowing infrastructure-less aeronautical network for ad-hoc networks between aircraft. With this in place it was envisioned to ensure high-capacity secure, future Air-Air services, such as ADS-B from aircraft to neighboring aircraft. Figure 6 depicts the overall idea illustrating how data can be transferred in ad-hoc network's manner from one aircraft to other stations (e.g., AS, GS).

III. LDACS's Cybersecurity Architecture

As described throughout Section II the following steps towards LDACS were designed, implemented, and performed:

- The system design and optimization via simulations including interference mitigation were the first step.
- The LDACS protocol design, starting from layer two in the ISO/OSI stack, is done.
- Navigation functionalities of LDACS were included and proofed and even flight-trialed.
- The LDACS system specification under the lead of EUROCONTROL and SESAR has been completed.
- From there, the technology was transferred to the industry (Frequentis, Rhode & Schwarz and LEONARDO).
- And lastly DLR performed an evaluation of the compatibility with other L-band systems.

As test were successful standardization of LDACS itself started in 2016 with ICAO in the working group ”ANB/AN: DCIWG PT-Terrestrial” [18]. As an important step, the LDACS Standards and Recommended Practices (SARPS) were agreed upon in October 2018. The plan for the future is to release guidance material by the end of 2022 in order to have LDACS applied 2024. Then LDACS will be the world's first realized true integrated CNS system.

Due to the fact that digitalization rises also in importance in aeronautical communication [1], [30], [34], security threats increase in parallel as pointed out in safety and security analyses [12], [20]. These results forced DLR to address this security issue for LDACS as soon as possible by drafting a cybersecurity architecture for LDACS as detailed described in [19]. As presented in [21] the SESAR 2020 Security Analysis (SecRAM) process in 2018/2019 revealed new findings on security threats (e.g., DoS on PHY layer, malicious operation software) and recommended a first set of algorithms overcoming them and improving LDACS. These recommendations were integrated into LDACS's cybersecurity architecture as described in detail in [21].

A. Security Features and Message Flow

Figure 5 illustrates the LDACS stack and as it can be seen in each stack component a feature for the realized cybersecurity architecture is included. These are the following seven functionalities [21]:

1) *Protection of Control Channels*
LDACS supports four channels dedicated for maintaining the link only. We recommend to further investigate lightweight cryptographic integrity and authenticity protection for the Random Access (RA), Common Control (CC) and Dedicated Control (DC) channel such as Lightweight Message Authentication Code (LMAC) [4] however the most important aspect is to protect the Broadcast Control (BC) channel as before an aircraft enters an LDACS cell it has to receive a beacon message by the GS. For this reason we recommend using a combined approach with digital signatures embedded in the broadcast control message by the GS and the Timed-Efficient Stream Loss-tolerant Authentication (TESLA) protocol [23].

2) *Trust*
Before establishing any kind of security and handing out any security relevant information (e.g.,such as identification information, cryptographic certificates) we have to rely on an overall structure that enables us to establish trust among entities. As LDACS and AeroMACS are both FCI candidates with AeroMACS already strongly deployed in China and an existing Public Key Infrastructure (PKI) in place [5] we can use the already established mechanisms of an ICAO trust bridge, with Digicert hosting the root Certificate Authority (CA) in San Diego USA and eonti being responsible for the rollout and distribution of certificates for LDACS. Ongoing investigations are undertaken checking applicability of newer approaches on trust like Blockchain based PKI and Keyless Signature Infrastructures with Zero Knowledge proofs for LDACS.

3) *Entity Authentication*
Signed Station-to-Station (STS) protocol [2] with preinstalled certificates on the end-entities is used for entity authentication. Post-Quantum schemes and Quantum-Key Distribution are under investigation.

4) *Key Negotiation*
The dual functionality of the STS protocol is used here.

5) *Key Derivation*
For session keys of arbitrary length with high entropy we recommend the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [17].

6) *Confidentiality Protection of Messages in Transit*
AES-256 in Galois Counter Mode (GCM) is recommended. It also covers integrity and authenticity protection of messages in transit with the same algorithm.

7) *Integrity and Authenticity Protection of Messages in Transit*
AES-256-GCM or a standard HMAC with hash-functions of the SHA3 family approach are recommended.

Figure 7 illustrates which tasks in which order is performed by which entity of the architecture linking it to the entities of the LDACS's protocol stack. GS and GSC securely set up a connection. Now the GS is identified, mutually authenticated and can start broadcasting its signed and TESLA protected beacon for all AS to receive. After that when an AS comes into the vicinity of a cell it can verify after the disclosure time of the TESLA keychain, that the messages are authentic and can verify the authenticity of the presumably broadcasting GS via its signature. With negotiated parameters for wireless transmission AS and GS can exchange messages and the AS transmits its identification and authentication related information to the GS which verifies them and if the verification is successful, forwards them to the GSC. The GSC also verifies the claim that the AS is actually the entity it claims to be and if successful, starts transmitting the required STS parameters to the AS. Now key negotiation, derivation and confirmation can be done between AS and GSC. As soon as this succeeds secure and, thus, encrypted, integer and authenticated communication can commence among authenticated parties.

IV. Implementation and Simulation

The security features and the respective message flow described in Section III-A were implemented in a Python event-based software simulation. The tool is capable of simulating world-wide air traffic movements, management of ATC/AOC data, cell coverage, and further features and is called FACTS2 [13]. FACTS2 is a service oriented simulation framework for aeronautical communication system evaluation developed and implemented by DLR. Due to the framework's structure a task separation becomes possible allowing natural parallelization at service level. With this strategy architectural complexity of software design stays low, and integration of existing software tolls is fostered. A comparison between data from real flight trials and data from the simulation showed, FACTS2 is able to simulate air traffic nearly as good as in reality and, thus, the best candidate to test the designed security features and message flows for LDACS's cybersecurity architecture.

A. Assumptions

For the final implementation of LDACS's cybersecurity architecture in the simulation tool the following assumptions were made:

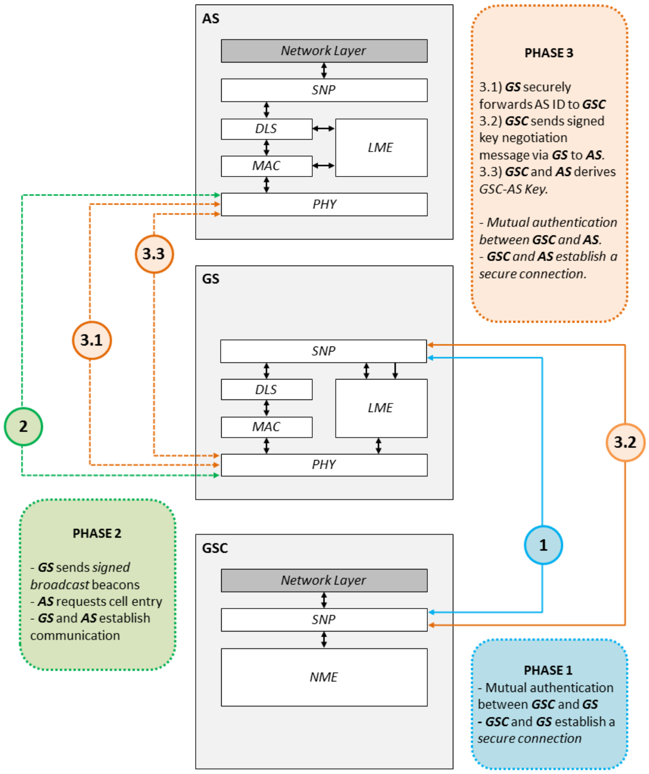

AS
Network Layer
SNP
DLS
LME
MAC
PHY
PHASE 3
3.1) GS securely forwards AS ID to GSC
3.2) GSC sends signed key negotiation message via GS to AS.
3.3) GSC and AS derives GSC-AS Key.
- Mutual authentication between GSC and AS.
- GSC and AS establish a secure connection.
3.3
3.1
GS
SNP
DLS
LME
MAC
PHY
2
3.2
PHASE 2
- GS sends signed broadcast beacons
- AS requests cell entry
- GS and AS establish communication
GSC
Network Layer
SNP
NME
1
PHASE 1
- Mutual authentication between GSC and GS
- GSC and GS establish a secure connection

Fig. 7. Steps performed to gain security in LDACS

(A1) The actual computation time takes no time in the simulation as it is negligible compared to the transmitting time even for the smallest frame in LDACS.

(A2) LDACS implements an Automatic Repeat Request (ARQ) protocol, thus if frames are lost due to simulated Bit-Error Rate (BER) the data is retransmitted as specified by the LDACS standard for acknowledged send mode.

(A3) The AS remain in the same range and, thus, the same BER (Bit Error Rate) is used for all scenarios, even though in reality the planes will approach the GS (signal improves, BER is decreasing) and leave the LDCAS cell (signal lessens, BER is increasing).

(A4) The packet generators use exponential distribution to match the requested load on the link, however only transmits dummy data of the actual length of real ATS or AOC data.

(A5) Certificates for end-entities were already locally stored and are not part of the STS message exchange to reduce the overhead of security data.

(A6) Before starting with the actual description, it is important to note that in our implementation the most trusted entity is regarded as "server" and the other one as "client". For example if GSC and GS communicate, the GSC is the server and the GS is the client. The resulting order of trustworthiness is then GSC $>$ GS $>$ AS.

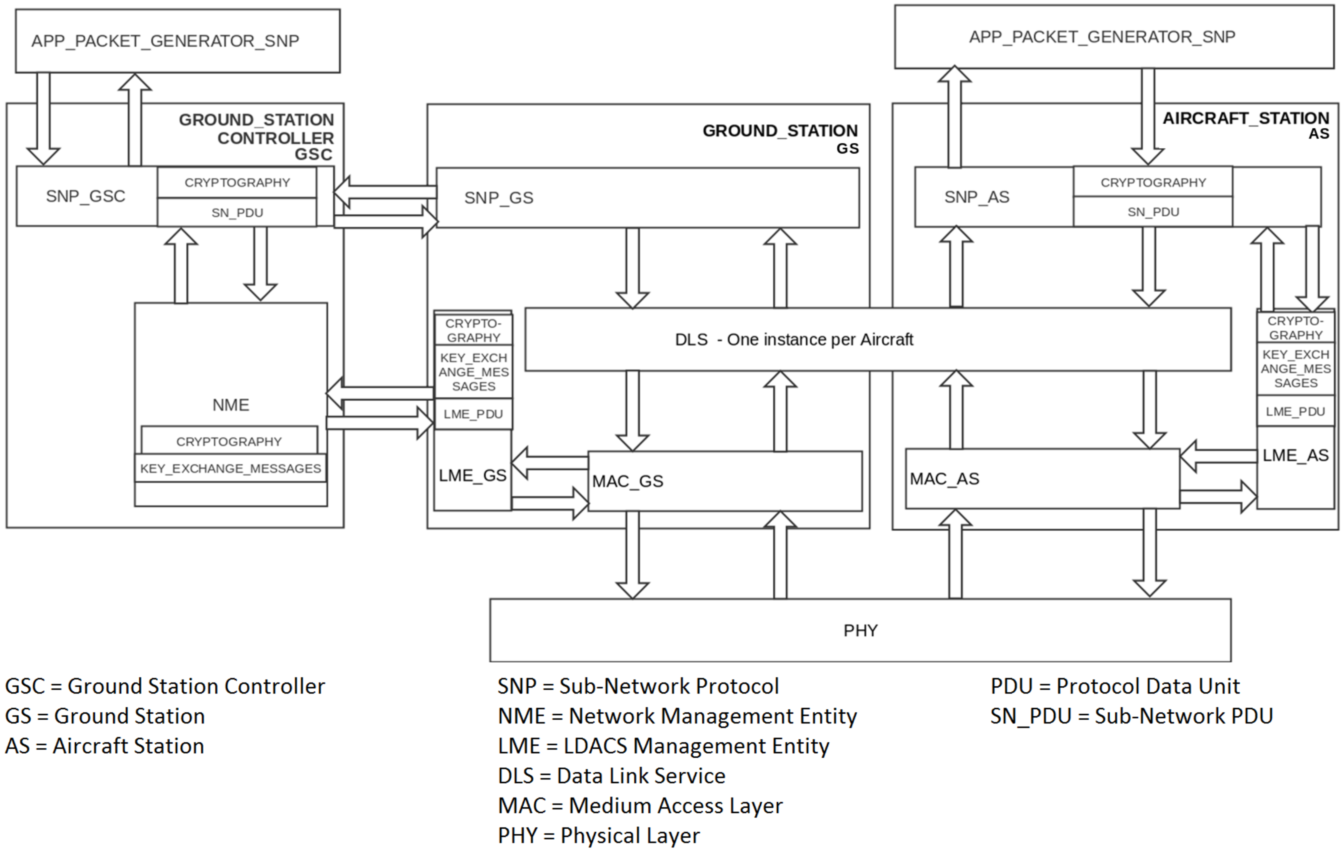


Fig. 8. Software implementation of the LDACS protocol with security additions

With the assumptions A1-A6 in place the existing simulation tool was extended for the evaluation of the message flow within the LDACS protocol stack. The extension includes the following and results in the data flow shown in Figure 8:

- There is a GSC, one GS, and up to 512 AS connecting to that GS, which in turn is linked to the GSC.
- The message exchange between GSC, GS, and multiple AS can be accurately depicted.
- Data packets are simulated by packet generators *(APP_PACKET_GENERATOR_SNP)* in 8 instead being sent from Air Traffic Network Service Providers (ANSP) or airlines in reality.

Important to know here, is that the general structure of classes of the protocol stack and the interactions between protocol layers are indications (ind) and requests (req), used to send messages back and forth. Usually a class starts with the initialization, summing up all required variables of that class. Then all necessary functions are listed, among them all req methods. Finally in a *run()* function, an infinite loop continues to wait for indications pointed at that respective entity and layer and, reacting to these indications, performs a certain action. Thus, we get the event based simulation. Each time a suitable message is received at a certain time, an action is performed.

B. Value Settings

With the adapted protocols and the transition from incoming data packets from the IP Layer (IPv6) to the SNP, we needed to adjust the STS protocol messages for the designed **key negotiation and entity authentication**. As we define the required certificates already to be stored upon the LDACS communication devices, we do not need to include these in the message exchange. Therefore, we can start with the `SignedClientHello` message, which has the structure and parameters selected as listed in Table II. For the `ServerHelloKeyExchange` message, depicted in Table III, we integrated also parts of the key exchange message to reduce the total amount of exchange packets. Regarding the two `KeyExchangeFinished` packets (cf. Tables IV and V) we follow STS message exchange without changes. These four messages of table II - table V are exchanged between the *NME* of the GSC and the *LME*s of AS and GS as depicted in Figure 8.

In the implementation we work with so called **Signed beacons**. Hence, for securing parts of the data channels, we suggest putting a signature in the BC slots in the BCCH channel together with the TESLA protocol, thus allowing incoming aircraft on the first receipt of a GS announcement the verification of their identity. The corresponding packet structure is shown in Table VII, with Figure 8 showing, this

TABLE II
SignedClientHello message

Field	Size	Description
TYPE	4 bit	SignedClientHello
ID	12 bit	Packet Identifier
UA	28 bit	Unique Address - Packet Sender Identifier
PRIO	4 bit	Priority of packet
RNC	256 bit	Random Number Client
SIGN	128 bit	Signature
GS_VAL	1 bit	Field containing information of GS verification status of AS.

TABLE III
ServerHelloKeyExchange message

Field	Size	Description
TYPE	4 bit	ServerHelloKeyExchange
ID	12 bit	Packet Identifier
UA	28 bit	Unique Address - Packet Sender Identifier
PRIO	4 bit	Priority of packet
RNS	256 bit	Random Number Server
G	2048 bit	Generator for cyclic group mod p
P	224 bit	Prime Number for cyclic group
GX	2048 bit	g^x, x chosen in secret by sender

TABLE IV
ClientKeyExchangeFinished message

Field	Size	Description
TYPE	4 bit	ClientKeyExchangeFinished
ID	12 bit	Packet Identifier
UA	28 bit	Unique Address - Packet Sender Identifier
PRIO	4 bit	Priority of packet
GY	2048 bit	g^y, y chosen in secret by sender
ENCSIGGYGX	256 bit	Signature of g^y, g^x encrypted with common key derived from message $key = (g^x)^y mod\ p$ exchange.

TABLE V
ServerKeyExchangeFinished message

Field	Size	Description
TYPE	4 bit	ServerKeyExchangeFinished
ID	12 bit	Packet Identifier
UA	28 bit	Unique Address - Packet Sender Identifier
PRIO	4 bit	Priority of packet
ENCSIGGXGY	256 bit	Signature of g^x, g^y encrypted with common key derived from message $key = (g^y)^x mod\ p$ exchange.

TABLE VI
SN_PDU message

Field	Size	Description
TYPE	4 bit	ACK/UNACK/MGMT
PID	5 bit	Packet ID
SC	3 bit	Service Class
SAC	28 bit	Subscriber Access Code
LEN	12 bit	Octets PDU
USER DATA	844-12108 bit	Payload (optionally encrypted)
MAC	128 bit	Integrity Checksum

TABLE VII
TESLA protected signed System Identification Broadcast message

Field	Size	Description
B_TYPE	4 bit	System Identification Broadcast
LEN	10 bit	Length given in bit
GS SAC	12 bit	GS Identifier - Identifier who sent the packet
VER	3 bit	Protocol Version
FLF	12 bit	Forward Link Frequency
RLF	12 bit	Reverse Link Frequency
MOD	1 bit	User-/Cell-specific ACM
CMS	3 bit	Coding and Modulation Scheme
EIRP	7 bit	GS Equivalent Isotropic Radiated Power
PAD	0 bit	Reserved
CRC-8	8 bit	Cyclic Redundancy Check
SIGN	128 bit	GS Specific Signature
MAC	128 bit	TESLA authenticated packet proof
TESLA_KEY	128 bit	TESLA key for respective interval

broadcast message can only be sent from the *LME_GS* and is received by the *LME_AS*.

All incoming data from the network will be encapsulated in so called **SN_PDUs**. The packet structure and its parameters is depicted in Table VI and only exchanged, with applied cryptographic mechanisms, between the *SNP*s of GSC and AS - as shown in Figure 8.

With the described messages in place, a message exchange can be performed enabling secure key negotiation, entity authentication and finally the confidential, integrity protected transmittance of user data.

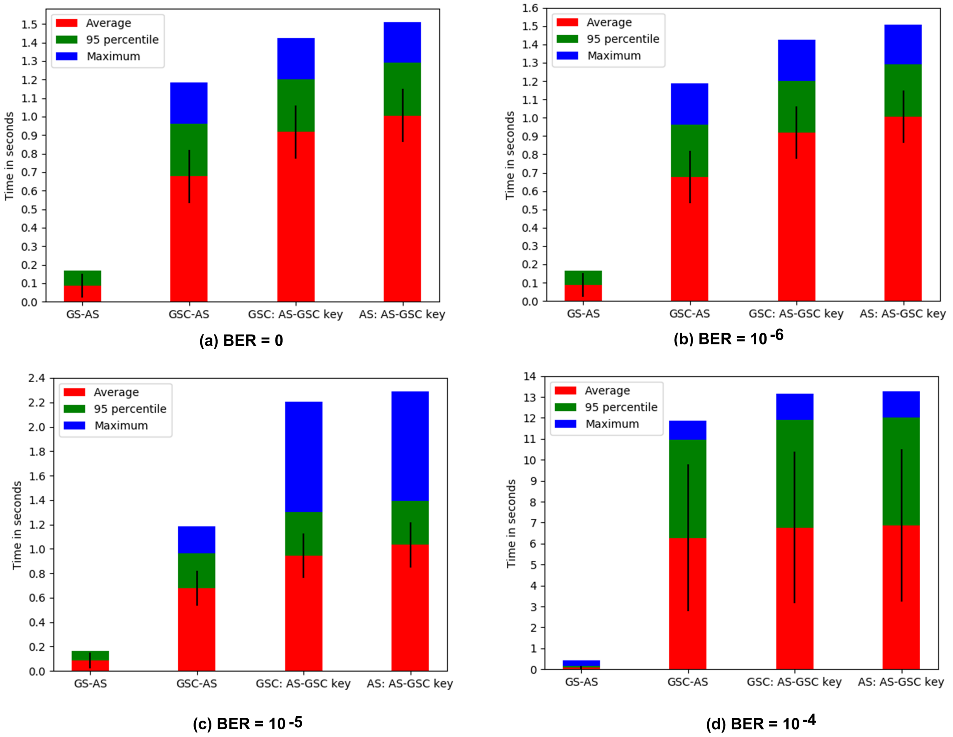
V. Evaluation

Before conducting flight trials we implemented the proposed cybersecurity architecture in software simulations. First evaluation of data showed promising results regarding the following points which are part of the objectives mentioned in the official LDACS SARPS (Standards and Recommended Practices) by ICAO [18]:

1) For time overhead added by the entity authentication, key agreement, negotiation and derivation, we wanted to show that it takes less than two seconds to securely connect an AS to the LDACS network.
2) Regarding data overhead by additional security we wanted to use less than five percent of additional user-data capacity.

A. Time Overhead by Security Additions

The time until an aircraft is authenticated by and to all other entities and until AS and GSC have a key, can be precisely measured when having many aircraft enter the cell and perform all the required operations. So we do not need actual data packets to be exchanged as we are focused on the first seconds of communication. We tested with a total number of 500 AS, each entering with two seconds of time margin to each other.



(a) BER = 0

(b) BER = 10 -6

(c) BER = 10 -5

(d) BER = 10 -4

Fig. 9. Duration of AS, GS and GSC mutual authentication, key negotiation and secure connection establishment time

Further we checked for different BERs, to measure the impact of the BER on performance. BER steps were chosen according to previous work [14], ranging from 0, 10^{-6}, 10^{-5} and10^{-4}. However the BER should only start to be noticeable around a BER of 10^{-5}. LDACS is designed for a BER up to 10^{-4} to work and on average, a BER of 10^{-6} is assumed [13]. With 500 ASs in place we observed that the FL-/RL-Load, the size of SN_PDU and the acknowledged transmission were either constant or irrelevant values and, thus, we decided to altered only the following parameters for additional trials:

- Simulation time = 500 seconds
- BER varies between the values 0, 10^{-6}, 10^{-5}, and 10^{-4}

Finally, we ended up with four simulation scenarios. Each one was performed ten times in order to receive reproducible results. We investigated how long the time spans are for (i) GS and AS connection, (ii) GSC and AS connection, (iii) GSC has derived the AS-GSC master key, and (iv) AS has derived the AS-GSC master key and key confirmation was performed in respect to the different BER. After those four steps were successfully performed key derivation takes place and a secure session can be established, which takes almost zero processing time thus we neglect the derivation times.

As the received measurements illustrated in Figures 9a and 9b prove, a BER of 0 or 10^{-6} has little effect on the overall connection time for establishing a secure link. With an increasingly bad channel and thus a higher BER of 10^{-5}, Figure 9c shows that on average the overall connection time remains braodly the same as with lower BER, however the longest connection times take already 50% more time than with 10^{-6} BER. In Figure 9d, we can see that LDACS was designed to operate up to a maximum of one bit error per 10,000 bit and, thus, the very high connection and security exchange times due to retransmissions and waiting times with a BER of 10^{-4} are not surprising. The most important detail here is, that a secure LDACS link can still be established under such bad channel conditions.

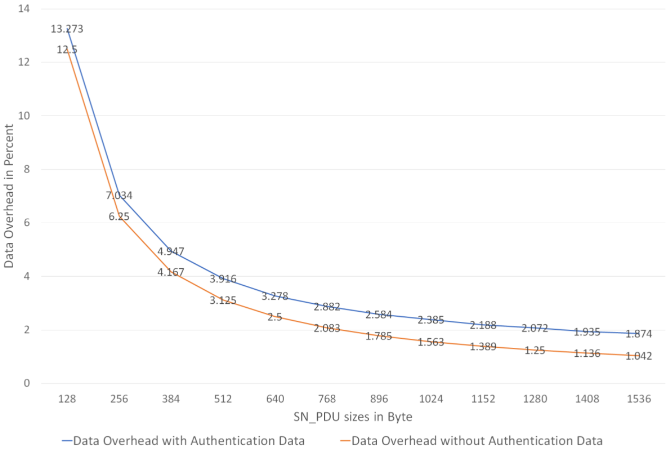


Fig. 10. Security data overhead on top of user data

B. User Data Overhead by Security Additions

Security data overhead is introduced by having additional authentication and key negotiation packets in the system and by using Message Authentication Codes (MAC) of 128 bit attached to data packets. Also additionally required retransmission depending on the BER due to larger or more packets due to security data overhead can have an impact on security data overhead. We use the following fixed parameters for our simulation:

- Number of AS is 100,
- 100 kbit/s for average FL/RL data throughput for all AS in one LDACS cell,
- 500 seconds simulation time,
- acknowledged transmission mode,
- BER = 10^{-5} to simulate ten times worse conditions than the average assumed BER, and
- MAC size of 128 bit

We alter only the size of the SN_PDUs between 128 byte, 256 byte, 384 byte, 512 byte, 640 byte, 768 byte, 896 byte, 1024 byte, 1152 byte,1280 byte, 1408 byte, and 1536 byte. Assuming on average, every 500 seconds a new key would have to be negotiated, as the AS leaves one GS range and enters another, we receive the security data overhead in dependence of the SN_PDU size.

In Figure 10 we see that depending on the size of SN_PDU packets the security overhead can range from 14% to 1%. This mostly results from the fix size of MACs attached to user data packets. To achieve our goal of less than 5% security data overhead, we recommend only using user data packets with a size larger than 256 bytes. Also we see that the average re-authentication time for moving nodes such as aircraft of 500 seconds only puts another 0.8% more security data on the link. Reducing this and the sizes of MACs will be critical to further reduce the security overhead on LDACS.

VI. Summary and Conclusion

In this paper we stated that security support is essential for future air traffic and related ATM. Therefore, we introduced a cybersecurity architecture for LDACS offering basic security functionalities (e.g., protection of control channels, trust. key negotiation) as described throughout Section III. Before the MICONAV flight campaign the designed and implemented solution was successfully tested within the FACTS2 simulation framework. With the gained results from several simulation runs we could prove that with the current implementation the overhead introduced by key exchange messages and Message Authentication Codes (MAC) applied to data packets is nearly negligible. We beat the two second mark for time overhead with the 95% percentile up until a BER of 10^{-5} and the five percent mark for data overhead with SN_PDU sizes larger than 256 bytes. At a realistic Bit Error Rate (BER) of 10^{-5}, the average connection time is 1.054 seconds. Assuming an internal data packet size of SN_PDUs larger than exactly 320 byte, we also beat the five percent margin, making the proposed security architecture viable.

As this work also presented a first proof-of-concept for the viability for the LDACS cybersecurity architecture, it will proof to be valuable input for the SESAR wave 2 specification of LDACS prior to its finalization and deployment as the terrestrial datalink for civil aviation.

During the MICONAV flight campaign additional data (e.g., evaluation on broadcast security of LDACS, use of Post-Quantum Cryptography (PQC) in digital aeronautical datalinks) was collected that will be further investigated and evaluated. In order to improve LDACS's cybersecurity architecture further we will have a closer look at post-quantum cryptography, a standalone trust solution for LDACS and additional protection for control messages and physical layer protection against jamming, spoofing and interfering with the datalink.

References

[1] A. Bilzhause, B. Belgacem, M. Mostafa, and T. Gräupl, "Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management," *Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 22–33, November 2017.

[2] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol," in *Public Key Cryptography*, ser. LNCS, vol. 1560. Heidelberg, Germany: Springer, March 1999, pp. 154–170.

[3] S. Brandes, M. Schnell, C.-H. Rokitansky, M. Ehammer, T. Gräupl, H. Steendam, M. Guenach, C. Rihacek, and B. Haindl, "B-VHF - Selected Simulation Results and Final Assessment," in *25th Digital Avionics Systems Conference (DASC).* New York, NY, USA: IEEE, October 2006, pp. 3A4/1–3A4/12.

[4] A. Chowdhury and S. DasBit, "LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network," in *Global Communications Conference*, ser. GLOBECOM. New York, NY, USA: IEEE, December 2015, pp. 1–6.

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

[6] M. Ehammer and T. Gräupl, "AeroMACS - An Airport Communications System," in *30th Digital Avionics Systems Conference (DASC).* New York, NY, USA: IEEE, September 2011, pp. 4C1/1–4C1/16.

[7] EUROCONTROL, "Communications Operating Concept and Requirements for the Future Radio System," EUROCONTROL/FAA, Brussels, Belgium, COCR 2, 2017 (accessed July 9, 2019). [Online]. Available: \url{https://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/communications/cocr-future-radio-system-v.2.pdf}

[8] EUROCONTROL Statistics and Forecast Service, "European Aviation in 2040 - Challenges of Growth," EUROCONTROL, Brussels, Belgium, Technical Report 2, 2018 (accessed July 5, 2019). [Online]. Available: https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/reports/challenges-of-growth-2018.pdf

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

[10] A. Filip and D. Shutin, "Ambiguity Function Analysis for OFDM-Based LDACS Passive Multistatic Radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 3, pp. 1323–1340, 2017.

[11] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, Eds., *LTE Security.* Hoboken, NJ, USA: John Wiley & Sons, August 2010.

[12] N. Giraudon, M. Iannes, S. Tamalet, M. Lehmann, S. Ben Mahmoud, N. Larrieu, A. Correas, and S. Fasetta, "Part 1 - AeroMACS Safety and Security Analysis, Part 2 - AeroMACS Security Analysis," Montreal, Canada, December 2014 (accessed July 9, 2019). [Online]. Available: \url{https://www.icao.int/safety/acp/ACPWGF/

ACP-WG-S-5/IP09%20-%20SESAR%20AeroMACS%20Safety%20and%20Security%20Analysis_.pdf}

[13] T. Gräupl, "FACTS2: Extended Simulation Framework for ATM Communication Demand Analysis of Europe," in *36th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, September 2017, pp. 1–8.

[14] T. Gräupl and M. Mayr, "Method to Emulate the L-band Digital Aeronautical Communication System for SESAR Evaluation and Verification," in *34th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, October 2015, pp. 1–18.

[15] T. Gräupl, N. Schneckenburger, T. Jost, M. Schnell, A. Filip, M. Bellido-Manganell, D. Mielke, N. Mäurer, R. Kumar, O. Osecha, G. Barrista, T. Bögl, and T. Richter, "L-band Digital Aeronautical Communications System (LDACS) Flight Trials in the National German Project MICONAV," in *18th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, June 2018, pp. 4A2/1–4A2/7.

[16] B. Haindl, C. Rihacek, M. Sajatovic, B. Phillips, J. Budinger, M. Schnell, D. Kamiano, and W. Wilson, "Improvement of L-DACS1 Design by Combining B-AMC with P34 and WiMAX Technologies," in *9th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, May 2009, pp. 1–8.

[17] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," RFC 5869 (Informational), Internet Engineering Task Force, May 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5869.txt

[18] V. Maiolla, "Working Groups and Panels Library - PT-T (Terrestrial) - LDACS," ICAO, July 2019 (accessed July 8, 2019). [Online]. Available: https://portal.icao.int/CP-DCIWG/ACPWGF/Forms/ACPWGT.aspx

[19] N. Mäurer and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis," in *18th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, April 2018, pp. 1A2/1–1A2–11.

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

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

[22] O. Osechas and G. Berz, "Improving the Availability of LDACS-based APNT with Air-to-Air Ranging," in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*. New York, NY, USA: IEEE/ION, April 2016, pp. 91–99.

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

[24] C.-H. Rokitansky, M. Ehammer, T. Gräupl, M. Schnell, S. Brandes, S. Gligorevic, C. Rihacek, and M. Sajatovic, "B-AMC A System for Future Broadband Aeronautical Multi-Carrier Communications in the L-Band," in *36th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, October 2007, pp. 4D2/1–4D2/13.

[25] M. Sajatovic, B. Haindl, U. Epple, and T. Gräupl, "Updated LDACS1 System Specification," German Aerospace Center (DLR), Oberpfaffenhofen, Germany, SESAR2020 PJ14-02-01 D3.3.010 00.01.01, 2017 (accessed July 9, 2019). [Online]. Available: \url{http://www.ldacs.com/wp-content/uploads/2014/02/LDACS1-Updated-Specification-Proposal-D2-Deliverable.pdf}

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

[27] M. Schnell, S. Brandes, S. Gligorevic, C.-H. Rokitansky, M. Ehammer, T. Gräupl, C. Rihacek, and M. Sajatovic, "B-AMC - Broadband Aeronautical Multi-carrier Communications," in *8th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, April 2008, pp. 4D2/1–4D2/13.

[28] M. Schnell, U. Epple, and F. Hoffmann, "Using the Future L-band Communication System for Navigation," in *11th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, May 2011, pp. J1/1–J1/12.

[29] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: Future Aeronautical Communications for Air-Traffic Management," *Communication Magazine*, vol. 52, no. 5, pp. 104–110, May 2014.

[30] M. Schnell, U. Epple, D. Shutin, N. Schneckenburger, and T. Bögl, "The German National Project ICONAV," in *13th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, June 2013, pp. 1–19.

[31] SESARJU, "High Performing Aviation for Europe," Brussels, Belgium, 2019 (accessed July 5, 2019). [Online]. Available: https://www.sesarju.eu/

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

[33] United States Department of Transport, "Modernization of U.S. Airspace - NextGen," Washington D.C., USA, June 25, 2019 (accessed July 5, 2019). [Online]. Available: https://www.faa.gov/nextgen/

[34] N. Zelkin and S. Henriksen, "L-Band Digital Aeronautical Communications System Engineering - Initial Safety and Security Risk Assessment and Mitigation," National Aeronautics andSpace Administration, TT Corporation Advanced Engineering & Sciences Division, Cleveland, OH, USA, NASA/CR-2011-216327, January 2011 (accessed July 5, 2019). [Online]. Available: https://archive.org/details/NASA_NTRS_Archive_20110005653