An overview of next-generation aviation cybersecurity

Daniel Rilegård
TDDD17 - Information Security 2021
Linköping University
Linköping, Sweden
danri396@student.liu.se

Ludvig Thor
TDDD17 - Information Security 2021
Linköping University
Linköping, Sweden
ludth083@student.liu.se

***Abstract*—The communication in aviation cybersecurity today is insecure. This means that data is sent unencrypted both over VHF radio and data links. To deal with this issue, a new system is currently under development that aims to improve the aviation cybersecurity situation. This system is referred to as FCI, Future Communications Infrastructure and consists of SatCom (satellite communication), AeroMACS (Aeronautical Mobile Airport Communication System) and LDACS (L-band Digital Aeronautical Communications System). The main difference in regards to communication between this new system and the old ones is that everything will be sent digitally over wireless technologies such as 4G/LTE. AeroMACS will handle the communications at the airport between ground stations and various devices on the surface. LDACS will handle the communication in air over busy areas with a lot of traffic and SatCom will handle communications across oceans and similar with less air traffic.**

To ensure secure communications, both LDACS and AeroMACS will have a robust Public Key Interface, PKI, which will handle certificates for entities and key derivation for keys that are used for encryption of sensitive data. AeroMACS already has a solution in place for PKI. The current plan for LDACS is to adopt the same solution as AeroMACS regarding PKI. For certificates, it is recommended to use X.509 certificates. They should either be installed directly on relevant hardware or distributed via ad hoc networks.

For LDACS, AES encryption standard is recommended for use to ensure confidentiality and HMAC with hash function SHA3 is recommended to ensure integrity of messages. This future solution should also be so called quantum proof, meaning that they are safe even from quantum computer attacks that might be possible in the future. It has been demonstrated that the AES-256 and SHA-3 algorithms are quantum proof which should make LDACS safe to use in the future but since AeroMACS uses AES-128 safety is not guaranteed.

I. Introduction

A. The problem in aviation cybersecurity today

Today, commercial aviation cybersecurity is using mostly old technologies such as VHF radio communication to relay information to pilots in the cockpits. There are more modern solutions that are used to some extent, such as CPDLC which is text communication sent over data links. The main problem with both of these solutions is that the communication between aircraft and ground stations is inherently insecure. This means that the traffic is sent unencrypted between aircraft and ground stations.

This makes the aircraft and the ground stations vulnerable to a number of attacks that can be performed by hackers. Proof-of-concept attacks have shown the possibility of several of these attacks in an application called ADS-B, a system for aircraft navigation. The background section will have more information about this.

Another issue is that the frequencies that are used today are simply too few and too crowded to be able to handle the aircraft communication traffic, which is expected to increase over the coming decades. There is a need for new technologies that deals with both the security and the bandwidth problem in aviation communications.

This paper reviews several of the currently used technologies as well as the upcoming future alternatives and evaluates the security functionality of the future alternatives.

Since the technologies are not fully developed yet, there are a lot of things regarding choice of algorithms and such that have not yet been completely decided on. There are however recommendations from knowledgeable researchers and developers in the industry.

B. Method

The main method of gathering information is to read papers related to and about aviation cybersecurity in order to understand the issues and present the current solutions for the problems.

C. Research questions

- How do the security mechanisms of LDACS and AeroMACS work?
- What are their respective strengths and weaknesses?
- What is their ability to interoperate?
- How do they compare to currently used technologies?

D. Related work

There are several papers that have been helpful when writing this paper. This technology is still in its infancy but there is still a lot of relevant information regarding the cybersecurity aspect of both AeroMACS and LDACS.

One example is *A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)* by

Nils Mäurer where he goes into great detail about the recommended practices for the LDACS cybersecurity architecture. He also writes about security objectives for LDACS and what technologies will support these functionalities. He also makes recommendations for encryption algorithms and certificates. This paper has been a great resource for understanding the ongoing development of LDACS. [1]

Another helpful paper is *L-band Digital Aeronautical Communications System (LDACS) draft-maeurer-raw-ldacs-06* by Mäurer et al. This paper goes into further detail on a lot of technical aspects regarding LDACS and was a great resource in conjunction with the previously mentioned paper. [2]

II. Background

A. Current technologies

1) ADS-B: Automatic Dependent Surveillance-Broadcast: ADS-B is a system for commercial aircraft navigation. It also has services for things like weather reports and traffic situation [3]. The navigation data includes for example aircraft position, velocity and identity. The main problem, and what this paper focuses on, is the fact that this data is sent unencrypted over data links. This makes it easy for legitimate actors to display the airplanes and their position, velocity and other interesting data. It also makes it easier for less legitimate actors to perform attacks against the system and the aircraft which might compromise security. In Security analysis of the ADS-B implementation in the next-generation air transportation system by McCallie et al. they go over several example attacks possible against ADS-B. One example of such an attack is Ground Station Target Ghost Inject where a attacker can put a fake aircraft on the display of a ground station by injecting false positional data. [4]

2) CPDLC: Controller–Pilot Data Link Communication: CPDLC is a system for communication between aircraft and Air Traffic Control (ATC) used as an alternative to Very High Frequency (VHF) voice radio transmissions. It consists of a two-way data-link system used mainly to transmit non-critical information such as various clearances, start-up messages and radio frequency assignments. Much of this traffic is sent terminal-to-terminal using predetermined phrases without any direct human involvement, but free-text messages can also be sent. This reduced human control has greatly decreased the risk of collision during flight due to pilots misunderstanding instructions sent via VHF. CPDLC should be considered an insecure mode of communication since it uses unauthenticated data links, which in combination with little direct human control makes eavesdropping or impersonating communications through replay attacks both possible and difficult to detect. A practical example of this is that CPDLC communications were successfully captured and read during an experiment at Stockholm Arlanda Airport using only basic tools in the form of an USB dongle as an radio scanner connected to a standard laptop PC [5]. [6][7]

Even though CPDLC is an insecure means of communication today, it will be part of LDACS in the future as the means of sending messages between ground stations and aircraft. In the LDACS realization, it will utilize the security functionality of LDACS to send secure messages between ground stations and aircraft. [2]

3) ACARS: Aircraft Communications Addressing and Report System: ACARS is a system used to communicate simple free-text digital messages between ATC and aircraft, status messages, and positional data when aircraft are outside radar coverage. ACARS contain no inherent security measures and messages are sent in plaintext which can be intercepted using any commercial radio receivers. Individual airlines have tried various methods to improve security, most commonly using custom formatting of the messages and simple encryption. [8]

B. Future alternatives

In this subsection we will review the possible future technologies used today in the aviation cybersecurity field.

1) FCI: Future Communications Infrastructure: To be able to handle the aircraft traffic today and in the coming decades there is a need for a new system that can support higher bandwidth and with better security solutions compared to the systems today. FCI is an infrastructure that will do just that. It is in its essence a new Internet Protocol Suite (IPS) system designed to be able to support Communication, Navigation and Surveillance (CNS) for aircraft by providing the necessary functionality regarding both digital and secure communications. FCI is supported by for example Eurocontrol, which is a civil-military organization dedicated to bring support to the aviation situation in Europe. They are not part of the European Union but the EU is, among other countries, a part of Eurocontrol. [9][10]

FCI is based on three different new technologies, AeroMACS, LDACS and SatCom(satellite communication with aircraft). This paper will focus on AeroMACS and LDACS.

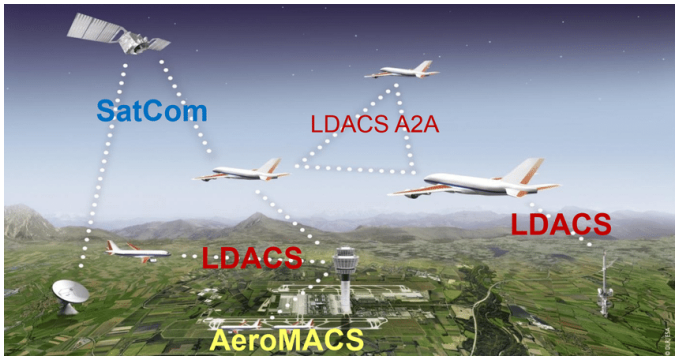

Fig. 1. FCI [9]

2) AeroMACS: Aeronautical Mobile Airport Communication System: In FCI, the role of AeroMACS is to provide high bandwidth IP Ground-to-Ground wireless communications mainly for use between devices on or near the airport surface. Continued development of AeroMACS is considered essential by EUROCONTROL, FAA and ICAO in order to provide new infrastructure for future growth in air traffic. [11]

The AeroMACS system is designed as a unifying standard for providing secure communication with a multitude

of different applications and is typically set up in the ATC tower. The effective range of AeroMACS is roughly 3 km and the wireless frequency spectrum that it works in is from 5091 MHz to 5150 MHz which is protected and requires a license to use. A few examples of possible uses are monitoring aircraft communication or security information, receiving data from various sensors and directing ground operations. Most of these different applications are divided into two categories; fixed and mobile assets, with fixed assets meaning applications communicating with stationary devices and mobile mainly regarding communication with vehicles on or near the airport surface. [11]

AeroMACS has been in development since 2007 and is based on the older WiMAX IEEE 802.16e wireless standard. This means that it will have the same security capabilities as 802.16e, enabling the use of a Public Key Infrastructure (PKI) for secure data exchanges over insecure networks and strong device-to-device encryption. [12][13]

3) LDACS: L-band Digital Aeronautical Communications System: The role of LDACS in FCI will be to provide communications between aircraft that are currently in the air and airports (long range terrestrial communications), as well as communication between different aircraft in the air, called Air-Air communications [9].

LDACS will be able to not only handle communications with ground stations and aircraft, but also handle navigation data. This means displaying for example the position, altitude and velocity of aircraft currently in the air. This ties into flight guidance which is explained below. [14]

LDACS will also handle flight guidance and will do so by using three different applications, Context Management (CM), CPDLC and Automatic Dependent Surveillance - Contract (ADS-C). The point of having a context manager is to have some kind of functionality that automatically sets up sessions for communications between ATC and aircraft. Today, the aircraft crew does this manually by changing VHF voice frequencies as the aircraft progresses in its flight. The second application, CPDLC, makes it possible to exchange messages over data links instead of voice over. This should result in a more reliable means of communication where there is less risk of misunderstandings than can occur when talking over voice radio. CPDLC is, like mentioned before, already in use in some cases but with the implementation of the FCI and LDACS it will be more widely used and also more secure than it is today. The final application mentioned, the ADS-C, will be responsible for reporting the current position of the aircraft and relay that information to the ATC. Together, these three applications will provide flight guidance in LDACS. [2]

The main difference between today's technologies and LDACS is that everything will be sent digitally over a wireless connection instead of VHF radio which is usually the means of communicating today. In order to make this kind of communication possible, technologies found in the 3G and 4G mobile networks are employed [9]. There are also other data links solution that exists today. One example of that is VDLM2. However, LDACS will be able to handle 50 times the amount of data compared to VDLM2 which makes communication over data links much more efficient and reliable. For ground to air communications, LDACS will be able to handle 315 kbit/s to 1428 kbit/s and for the reverse link, air to ground, it will be able to handle 294 kbit/s to 1390 kbit/s. The exact amount it is able to handle will depend on how the system is configured regarding coding and modulation. [2]

4) PKI: Public Key Infrastructure: PKI is a system for deriving and handling public keys that are used to authenticate entities. Each entity, or user, has their own public key which is tied to the entity via a so called certificate. This certificate is handled by a trusted Certificate Authority (CA). If two parties want to exchange sensitive information then they can use a PKI to do that. An algorithm such as Diffie Hellman can be used to generate a secret key that is known only to the two parties. They can then encrypt data and send it to the other party which can then decrypt it with the key same key. The PKI is an important concept for LDACS and AeroMACS to ensure a secure communication link. The evaluation chapter will go more in depth about what have been done as well as what is to be done in regards to key generation. [15]

III. Security comparison and evaluation

A. AeroMACS cybersecurity

AeroMACS is not intended to replace any specific system currently used. It is rather meant as a unifying standard and to complement VHF voice communications in order to alleviate frequency congestion by providing additional spectrum band frequencies for aircraft close to airports to receive important information in text format. By serving as a common framework that is designed to allow various systems to easily interoperate in a secure manner, adopting AeroMACS will lead to improvements regarding all three parts of information security CIA; Confidentiality, Integrity and Availability. [13]

ICAO have stated several Standards and Recommended Practices (SARPS) for AeroMACS regarding what is necessary to ensure system security [16]:

1) AeroMACS shall provide a capability to protect the integrity of messages in transit.
2) AeroMACS shall provide a capability to ensure the authenticity of messages in transit.
3) AeroMACS shall provide a capability to protect the availability of the system.
4) AeroMACS shall provide a capability to protect the confidentiality of messages in transit.
5) AeroMACS shall provide an authentication capability.
6) AeroMACS shall provide a capability to authorize the permitted actions of users of the system.
7) If AeroMACS provides interfaces to multiple information domains, AeroMACS shall provide capability to prevent intrusion from lower integrity information domain to higher integrity information domain.

Confidentiality is improved by ensuring that wireless communications are done over protected frequencies and are properly encrypted according to number 4.

Number 1, 2, 5, 6 and 7 deals with data integrity, mainly by protecting message integrity and ensuring communication authenticity. The encryption done by using a PKI also ensures data integrity since it prevents tampering by third parties.

Functions to guarantee availability will also be a part according to number 3. The overall availability of communications with aircraft is also improved due to providing additional channels for data transfer in the high-traffic airspace near airports. [13]

B. LDACS cybersecurity

As previously mentioned, the problem with today's aviation cybersecurity is that it is not very secure. Data is sent over unencrypted radio channels or data links. LDACS aims to improve the cybersecurity of this communication by adhering to the following 8 objectives which are defined by the official ICAO SARPS [2]:

1) LDACS shall provide a capability to protect the availability and continuity of the system.
2) LDACS shall provide a capability including cryptographic mechanisms to protect the integrity of messages in transit.
3) LDACS shall provide a capability to ensure the authenticity of messages in transit.
4) LDACS should provide a capability for nonrepudiation of origin for messages in transit.
5) LDACS should provide a capability to protect the confidentiality of messages in transit.
6) LDACS shall provide an authentication capability.
7) LDACS shall provide a capability to authorize the permitted actions of users of the system and to deny actions that are not explicitly authorized.
8) If LDACS provides interfaces to multiple domains, LDACS shall provide capability to prevent the propagation of intrusions within LDACS domains and towards external domains.

If LDACS follows these objectives, it would mean that it deals with CIA in an appropriate way. For example, number 1 ensures that LDACS keeps the system up and running which would deal with availability. Number 3 deals with integrity, so that the recipient knows that the message they received was not tampered with in any way. Number 5 deals with confidentiality, basically making sure that sensitive data can not be read by another party which should not have access to that data.

Another paper lists these seven functionalities that the LDACS cybersecurity architecture will be supported by. [9]:

1) Protection of Control Channels
2) Trust
3) Entity Authentication
4) Key Negotiation
5) Key Derivation
6) Confidentiality Protection of Messages in Transit
7) Integrity and Authenticity Protection of Messages in Transit

The key negotiation and derivation will be handled by the PKI, which is written about in more detail later on in the paper. Entity authentication is also a part of the PKI, but has more to do with certificates and how they are handled. To ensure that the confidentiality of the messages is protected in transit, the encryption algorithm that is recommended to use for LDACS is AES, Advanced Encryption Standard. This is virtually impossible for modern computers to break in a reasonable time frame and would mean that the confidentiality of messages is going to be protected [1]. In order to confirm that the integrity of the messages is intact, HMAC or a similar technology will be recommended for use in LDACS. HMAC creates a hash of the message and is sent together with the message. Upon arrival, the recipient can recalculate the hash and compare them. If the hashes do not match then someone has tampered with the message.

C. PKI and entity authentication for AeroMACS and LDACS

AeroMACS already has a solution in place for a PKI. In the AeroMACS PKI solution there are first of all the so called global root Certificate Authority which are signed and issued to each airplane/device manufacturer or operator. The root CA is distributed to and trusted by all other devices on the network in order to make interoperability possible. The certificates are for this purpose signed using a SHA-256 hash to prove authenticity. Below the root CA is several layers of certificates to ensure that the Certificate Policy (CP) is followed. This policy defines both the operational and procedural requirements that certificate recipients must adhere to. The AeroMACS PKI CP will provide the following security functions [1][17]:

1) Key generation and storage
2) Certificate generation, modification, re-key, and distribution
3) Certificate Revocation List (CRL) generation and distribution
4) Directory management of certificate related items
5) Certificate token initialization, programming, and management
6) System management functions to include security audit, configuration management, and archive

Keys used to authenticate communications over AeroMACS will be managed by an improved Privacy Key Management protocol (PKMv2) which uses X.509 certificates. These certificates are unique for each device and are either preinstalled by the manufacturer or distributed via ad hoc networks. They contain a public key and the MAC address of the associated device/operator, and can be encrypted using either the EAP or RSA method or a combination of the two. The public key is used to establish the initial server/device trust and to create Security Associations (SA) which are secrets shared by both parts. The SA is then used together with encryption to encrypt transmitted data. The master public keys are managed by ICAO in a Public Key Directory (PKD) which acts as a central repository for validation and safe distribution of certificates[18]. The public and private device keys will each be valid for a maximum of five years. [17] [13]

Traffic encryption by PKMv2 is done using AES-128 in CCM mode, enabling per packet encryption. In addition a unique nonce is added to each packet to protect its integrity and harden against replay attacks. [13]

The current goal for LDACS is to align the solution with the AeroMACS solution. To do this, X.509 certificates are proposed to be used for LDACS as well. As with AeroMACS, these certificates will either be distributed via ad hoc networks or simply pre-installed on the hardware. [1]

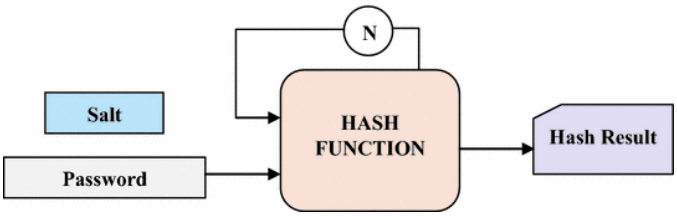

Fig. 2. Example of a KDF

In order to derive new keys to secure the LDACS session, there is a need for a key derivation function (KDF). The proposal from Mäurer is to use the function known as HKDF. It is a KDF that is based on HMAC. [1]

D. Quantum Proof

Many algorithms that are used today for encrypting data can not, in practice, be broken by an attacker. At least not within a realistic time frame. This is simply due to the large amounts of calculations that needs to be made which is infeasible for modern computers. In the future however, with quantum computers on the horizon, this assumption might be put into question since quantum computer can perform calculations much more efficiently than modern ones. Despite of this, Mahto et al. showed in The AES-256 Cryptosystem Resists Quantum Attacks that the AES-256 encryption standard, which is proposed to be used for LDACS, resists quantum attacks. It has also been shown that the algorithm SHA-3, which is proposed to be used with HMAC in LDACS, is also quantum proof. [19]

This should mean that even in a future with quantum computers, the infrastructure would still be safe from those kind of attacks and the confidentiality and integrity of messages would still be protected. [20]

Since AeroMACS uses AES-128 to encrypt traffic, there is reason to be concerned for quantum resistance for AeroMACS, since it has only been shown that AES-256 is quantum proof. It is assumed here that AeroMACS should not be considered quantum proof according to the previous information.

E. Interoperability

In order to implement LDACS and AeroMACS and make them function together in the real world, there is a need for a new system which makes this possible. That system is FCI. In this system, AeroMACS will handle the communications on the airport between the ground stations and the aircraft before lift off. LDACS will then handle the communications while in the air, mostly in more dense traffic areas. SatCom will handle large coverage areas such as oceans.

AeroMACS and LDACS will share the security implementations regarding for example the PKI. As mentioned previously, they will be using the same X.509 certificates for entity authentication as well.

Loung et.al. looked at ways to improve the handover aspect of aviation networks. Since several radio technologies are used and the aircraft are going at high speeds, there is a risk for packet loss during handovers attempts. They showed with an experimental implementation of the Locator ID Separation Protocol (LISP) and Random Linear Network Coding (RLNC) over an SDN-based architecture that it was possible to improve the performance during the handover by using these technologies. [21]

F. Potential issues

While implementing AeroMACS should be a much needed upgrade to airport infrastructure there are a few weaknesses that should be considered. While AeroMACS has an effective maximum range of around 3 km, the data transfer capacity drops as you move away from the transmitter. For this reason several overlapping transmitters are placed at even intervals along runways and similar where mobile devices such as aircraft and service vehicles typically moves. This allows the vehicles to continually change the transmitter they connect to in order to get the best connection possible. An issue where the Round Trip Time (RTT) e.g. the time for a sent package to receive an answer, spikes during this change of transmitter have been noticed during field tests. This is suspected to be due to timeout thresholds not being configured properly which leads to lost packets sent at the moment of transmitter handover waiting to be returned for too long. In order to prevent this issue it will be important for the various applications using AeroMACS to set appropriate values for their timeout thresholds. [22]

Another issue is that if the aviation traffic becomes encrypted in the future, it might make it more difficult for flight traffic applications online to display interesting information such as current flights in the air and their destinations. This could mean that those kind of operations might simply not be possible in the future. It could be possible to for example share the data with trusted companies but that would also mean another security risk which may not be worth it.

IV. Discussion

This paper is a theoretical paper in nature which means that the primary method of gathering information was to read research articles and other publications related to the issue of aviation cybersecurity. Due to this it was important to find papers of good quality to base the paper on. The majority of the content that was written was based on a few papers written by researchers (such as Nils Mäurer) whom are currently working on developing the cybersecurity infrastructure of LDACS. These papers were very helpful when it came to

understanding the issues with aviation cybersecurity and also understand what solutions are being proposed today.

Since the technologies are still in development, there are some things related to the cybersecurity aspect that are not very clear. A lot of the information regarding choice of encryption algorithms and similar are still only proposals and not final, since there is not really a final product yet. This means that some things might possibly be changed later on, such as policies and algorithms.

However, there is probably not a great reason to be concerned with this since the proposed algorithms are fairly standard and even if the recommendations were to be changed, the underlying functionality would most likely stay the same. If some things were to change, it would probably be towards an even better solution.

It was generally more difficult to find relevant information about AeroMACS compared to LDACS. LDACS seemed to have more comprehensive papers written about it by the researchers working closely on it. One example is the SARPS for either system. For LDACS they could be found in the paper *L-band Digital Aeronautical Communications System (LDACS) draft-maeurer-raw-ldacs-06* while it was very difficult to find the finalized ones for AeroMACS. The source used for AeroMACS is therefore an earlier draft of proposed standards and practices which still should at least be similar to the final ones.

V. Conclusions

The goal of this paper was to evaluate the future alternatives to the current aviation communication systems. In the background section, there is an overview of the current technologies and some examples of why they are not sufficient at providing a secure and reliable communications standard both for current day and in the future. The main issue is that data is sent unencrypted over either VHF radio or insecure data links. This opens the systems up for network attacks. The solution to these problems is what is referred to as FCI which consists of three different systems, SatCom, AeroMACS and LDACS. They will work together to provide a secure communications infrastructure that will be sufficient for decades to come.

This paper also discusses in detail the cybersecurity architecture for AeroMACS and LDACS which will ultimately be responsible for making sure that the communications are in fact secure. Encryption algorithm AES will be recommended to ensure the confidentiality of messages and for at least LDACS hashing algorithm SHA-3 will be recommended to be used together with HMAC to ensure the integrity of messages.

It is also important to have a robust PKI for generating keys. AeroMACS already has a solution in place and LDACS is expected to adopt the same solution. This solution includes X.509 certificates which will be installed directly on relevant hardware or via ad hoc. The certificates makes it possible to authenticate entities in the system to make sure that entities can be trusted. There is also a need for some kind if key derivation function (KDF). HKDF is proposed to be used here which is a KDF based on HMAC.

This paper also investigated whether or not AeroMACS and LDACS will be quantum proof. This means being able to resist attacks from future quantum computers. Two papers are discussed which showed that the algorithms AES-256 and SHA-3 both are quantum proof which means that at least LDACS will be quantum proof. There is a need to question the quantum proof of AeroMACS since it is not confirmed that AES-128 will be quantum resistant.

In summary, the current systems for aviation communications are insecure and lacks bandwidth. The future alternatives that are on the horizon promises to fix both of these issues making the aviation cybersecurity situation much more secure and robust than it is today.

References

[1] Martin Strohmeierr and Vincent Lenders. “A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)”. In: *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*. 2018. DOI: 10.1109/DASC.2018.8569878.

[2] Nils Mäurer, Thomas Gräupl, and Corinna Schmitt. “L-band Digital Aeronautical Communications System (LDACS) draft-maeurer-raw-ldacs-06”. In: *IETF* (2020).

[3] *Automatic Dependent Surveillance-Broadcast (ADS-B)*. https://www.faa.gov/nextgen/programs/adsb/. Accessed: 2021-04-20.

[4] A. Roy. “Security analysis of the ADS-B implementation in the next generation air transportation system”. In: *International Journal of Critical Infrastructure Protection*. Vol. 4. 2. 2011, pp. 78–86. DOI: 10.1016/j.ijcip.2011.06.001.

[5] André Lehto et al. “CONTROLLER PILOT DATA LINK COMMUNICATION SECURITY: A PRACTICAL STUDY”. In: (2021).

[6] Martin Strohmeier et al. “On Perception and Reality in Wireless Air Traffic Communication Security”. In: *IEEE Transactions on Intelligent Transportation Systems* 18.6 (2017), pp. 1338–1357. DOI: 10.1109/TITS.2016.2612584.

[7] Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. “Controller–Pilot Data Link Communication Security”. In: *Sensors* 18.5 (2018). ISSN: 1424-8220. DOI: 10.3390/s18051636. URL: https://www.mdpi.com/1424-8220/18/5/1636.

[8] A. Roy. “Secure aircraft communications addressing and reporting system (ACARS)”. In: *20th DASC. 20th Digital Avionics Systems Conference (Cat. No.01CH37219)*. Vol. 2. 2001, 7A2/1–7A2/11 vol.2. DOI: 10.1109/DASC.2001.964182.

[9] Nils Mäurer, Thomas Gräupl, and Corinna Schmitt. “Evaluation of the LDACS Cybersecurity Implementation”. In: *AIAA/IEEE 38th Digital Avionics Systems Conference (DASC) 2019*. 2019. DOI: 10.1109/DASC43569.2019.9081786.

[10] *Future communications infrastructure and multilink for the long term*. https://www.eurocontrol.int/function/future-communications-infrastructure-and-multilink-long-term. Accessed: 2021-04-20.

[11] *AeroMACS WiMAX Forum Initiative*. https://wimaxforum.org/Page/AeroMACS/. Accessed: 2021-04-24.

[12] *WiMAX Forum Security - PKI for WiMAX and WiGRID Devices*. https://wimaxforum.org/Page/Security. Accessed: 2021-04-27.

[13] Stuart Wilson. "The network security architecture and possible safety benefits of the AeroMACS network". In: *2011 Integrated Communications, Navigation, and Surveillance Conference Proceedings*. 2011, pp. D5-1-D5–9. DOI: 10.1109/ICNSURV.2011.5935269.

[14] *LDACS White Paper – A Roll-out Scenario*. https://www.ldacs.com/wp-content/uploads/2013/12/ACP-DCIWG-IP01-LDACS-White-Paper.pdf. Accessed: 2021-04-20.

[15] Radia Perlman. "An overview of PKI trust models". In: *IEEE Network* (1999).

[16] ICAO. "WP01 ACP WG S March telecon Draft AeroMACS SARPS". In: Mar. 2014.

[17] Brian Crowe. "Proposed AeroMACS PKI specification is a model for global and National Aeronautical PKI Deployments". In: *2016 Integrated Communications Navigation and Surveillance (ICNS)*. 2016, pp. 1–19. DOI: 10.1109/ICNSURV.2016.7486405.

[18] *ICAO-ePassport Basics*. https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx. Accessed: 2021-05-24.

[19] Jan Czajkowski. "Quantum Indifferentiability of SHA-3". In: *QuSoft, University of Amsterdam* (2017).

[20] Sandeep Kumar Rao et al. "The AES-256 Cryptosystem Resists Quantum Attacks". In: *International Journal of Advanced Research in Computer Science* (2017).

[21] Doanh Kim Luong et al. "Seamless handover in SDN-Based Future Avionics Networks with Network Coding and LISP Mobility Protocol". In: *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)* (2019).

[22] Junichi Naganawa et al. "An experimental evaluation on handover performance of AeroMACS prototype". In: *2016 Integrated Communications Navigation and Surveillance (ICNS)*. 2016, pp. 2C1-1-2C1–10. DOI: 10.1109/ICNSURV.2016.7486331.