Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis

Nils Mäurer, German Aerospace Center, Oberpfaffenhofen, Germany
Corinna Schmitt, Research Institute CODE, Bundeswehr University Munich, Germany

Abstract

Currently Communication Navigation and Surveillance (CNS) in civil aviation are undergoing huge changes in the framework of the European SESAR and the US NextGEN research initiatives. One goal is to develop the Future Communication Infrastructure (FCI) for civil aviation, consisting of AeroMACs for airport communications, SatCOM for remote domains, and LDACS for long-range wireless digital communications. The trend towards digitalization is supposed to solve the problems of capacity shortage, frequency saturation and automated data processing. Due to the digitalization process in communication itself and especially in critical infrastructure a strong request for cybersecurity support was raised. Therefore, a threat-and-risk analysis for LDACS was performed resulting in a first cybersecurity architecture specification draft. This paper goes one step further, presenting a suitable set of algorithms and protocols for security support for LDACS. The set is evaluated performance and security wise to match the cybersecurity architecture specification identified in earlier work.

1. Introduction

Worldwide civil air traffic is expected to grow by 84% until 2040 compared to 2017 [1]. Thus, legacy systems in air traffic management (ATM) are likely to reach their capacity limits and the need for new aeronautical communication technologies becomes apparent [1, 2, 3]. Especially problematic is the saturation of VHF band in high density areas in Europe, the US, and Asia [4, 5] calling for suitable new digital approaches such as AeroMACS for airport communications, SatCOM for remote domains, and LDACS as long-range terrestrial aeronautical communications system.

Making the frequency spectrum's usage more efficient a transition from analogue voice to digital data communication [2, 4, 5] is necessary to cope with the expected growth of civil aviation and its supporting infrastructure. A promising candidate for long range terrestrial communications, already in the process of being standardized in the International Civil Aviation Organization (ICAO)[1], is the L-band Digital Aeronautical Communications System (LDACS) [4, 6, 7]. LDACS is a terrestrial digital wireless communication system for civil operational aeronautical safety-of-life communication and based on 3G and 4G technologies, adapted for safety critical infrastructure requirements and deployed as an inlay system in the L-band next to Distance Measuring Equipment (DME) [4, 7, 8].

With the augmentation of analogue systems by digital substitutes and the related trend towards an increased autonomous data processing as justified in [1, 3], LDACS requires a thorough cybersecurity analysis and cybersecurity architectural design in its standards [6], similar to the ones used in 3G, 4G or AeroMACS [4, 9, 10, 11] in order to be successfully deployed. In previous work [4, 12, 13] a draft of the envisioned cybersecurity architecture for LDACS was announced in the community. It specifically regards special requirements of the LDACS environment such as narrow frequency ranges, and limited bandwidth. Concerning security support, especially for data transfer, it was already recommended to investigate for solutions with reasonable low overhead in order to be resource-efficient and building a key incentive for the envisioned LDACS security specification and standardization.

The main objective of this paper is to evaluate the effectiveness of the earlier proposed LDACS cybersecurity architecture with a suggestion of different algorithms and protocols for security support. The evaluation focuses on performance and robust-

[1] ICAO – Responsible for establishing international standards for civil aviation, ensuring the safe growth and standardization of international air transport.

ness analysis comparing LDACS implementations with and without security additions. Thus, Section 2 presents the envisioned multilink concept by DLR, supported within SESAR [2], including background information about LDACS leading to LDACS's cybersecurity architecture in Section 3. A threat-and-risk analysis is presented throughout Section 4 before concluding the paper in Section 5.

2. Networking the Sky

The European initiative Single European Sky (SES) started in 2004 with its goal to unify all European aeronautical sectors founded the accompanying Single European Sky ATM Research (SESAR) initiative. Within this large European research endeavor and the US pendant Next generation national Airspace Systems (NextGen), new broadband digital data link technologies for air traffic management are currently in development [14, 15, 16, 17, 18, 19, 20].

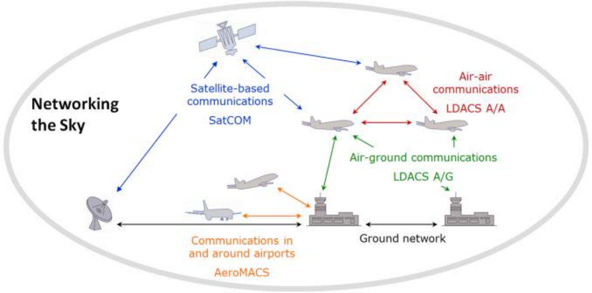
Networking the Sky
Satellite-based communications
SatCOM
Air-air communications
LDACS A/A
Air-ground communications
LDACS A/G
Communications in and around airports
AeroMACS
Ground network

Figure 1: DLR's "Networking the Sky" concept

Figure 1 illustrates the relationship between the different components building DLR's "Networking the Sky" concept [21, 22] including AeroMACS for near airport communications [10, 23, 24], SatCOM for oceanic, remote and polar domains [20, 25], and LDACS A/G for en-route terrestrial long-range communications [5, 6, 22, 26]. The scope of this paper focuses only on the LDACS A/G data link keeping the other communication ways and requirements in mind for potential further investigations and extensions for cross interactions.

The development of LDACS started 2007 in cooperation between the German Aerospace Center (DLR), Frequentis AG, and the University of Salzburg in Austria with its origins in merging parts of the B-VHF [17], B-AMC [26], TIA-902 (P34), and WiMAX IEEE 802.16e technologies [9, 24].

Challenging for any kind of specification in this application area are the diversity of entities involved and their individual requirements and specifications, especially on handling a high number of communication ways.

An LDACS network consists of three main entities: Aircraft Station (AS), Ground Station (GS) and Ground Station Controller (GSC) as illustrated in Figure 2. One GS can serve a total of 512 aircrafts and is in charge of maintaining a continuous data stream in the Forward Link (FL) [6]. In comparison to FL the involved Reverse Link (RL) is structured in individual bursts of data from each aircraft and, thus, for each RL communication the AS first needs to request the respective resource allocation within its cell from the GS, in order to send. Several GSs are linked to one GSC, forming an LDACS sub-network. The GSC in turn, is the link to the Aeronautical Telecommunications Network (ATN), for direct data transfer between air traffic control and aircraft.

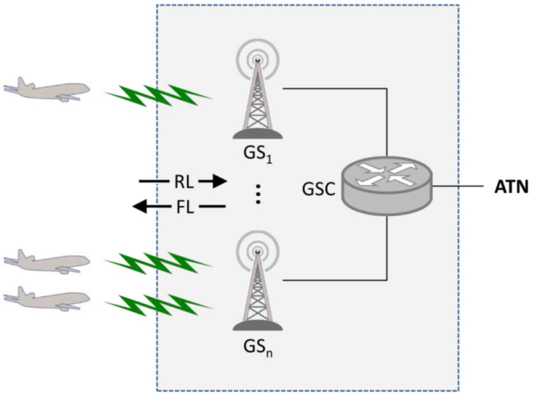

Figure 2: Entities of LDACS network

The LDACS protocol stack shown in Figure 3 supports data and voice communications. Data is split into user (e.g., ATM specific service data) and control data (e.g., link maintenance data) and we differentiate between Service Data Unit (SDU) and Protocol Data Unit (PDU). A SDU only consists of payload, carrying user or control data only. A PDU however is formed with a header, the actual payload (SDU) and it is possible to attach a trailer, Frame Check Sequence (FCS), Message Integrity Code (MIC), Padding etc.. LDACS's physical layer (PHY) transports user data in so-called DATA packet data units (PDUs), and control data in CC/DC PDUs to the Medium Access

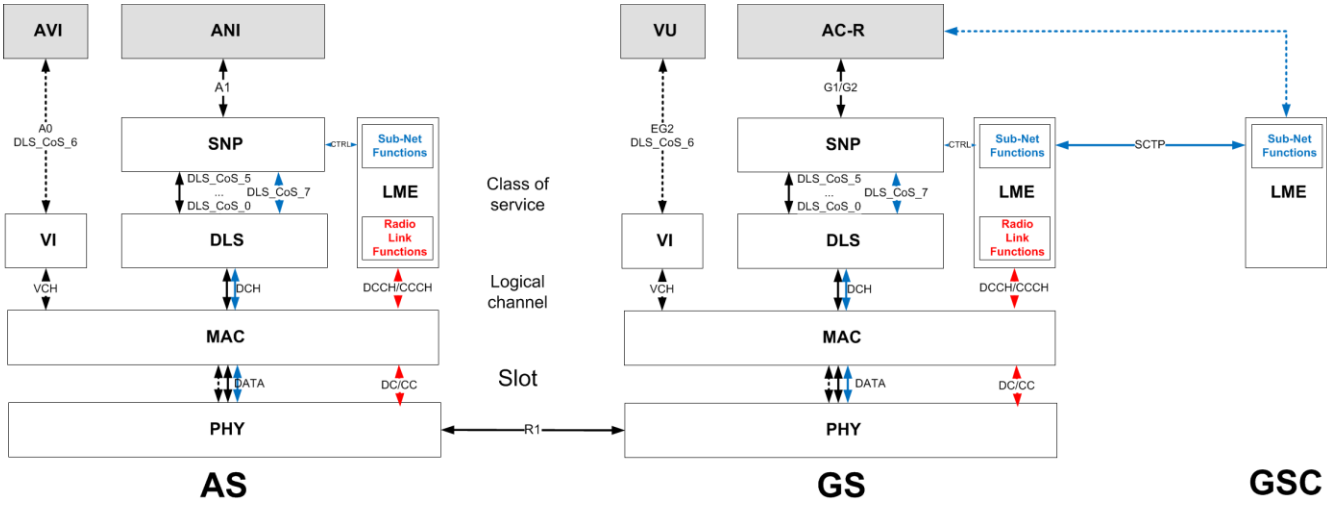

Figure 3: Interaction of all LDACS entities with their respective protocol stacks [6]

Control layer (MAC). On the MAC user data is sent in the logical Data Channel (DCH) to the Data Link Service (DLS) layer, while control data for maintaining radio link functions is forwarded to the LDACS Management Entity (LME) in the Common/Dedicated Control Channel (C/DCCH). However, MAC also supports two more control channels: (1) the Random Access Channel (RA), which AS can use to request access to the LDACS cell and (2), a Broadcast Channel (BC) used by the GS to announce their existence to incoming aircraft. Another channel used on MAC is the Voice Communication Channel (VCH) carrying voice messages via DLS Class of Service (CoS) 6 to the Aircraft Voice Interface (AVI) on the AS and to the Voice Unit (VU) on the GS. All logical communication channels are shown in figure 4.

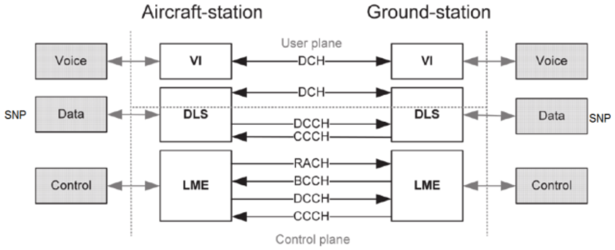

Figure 4: Overview of LDACS logical channels for user data (DCH) and control data (BCCH, RACH, CCCH, DCCH) [6]

After passing the MAC and being put into their respective logical channel, data is split now on the DLS into seven priorities DLS_CoS_0-7, with zero being the lowest priority and seven the highest (e.g., for safety critical messages). Above the DLS comes the Sub-Network Protocol (SNP), which communicates to the LME via control (CTRL) messages (e.g., for key handover LME to SNP) in the Sub-Network of the LDACS cell. AS and GS communicate via the radio link R1. GSC and GS mainly communicate via the Stream Control Transmission Protocol (SCTP). Hence, several AS are connected wirelessly to a GS, which in turn communicates via SCTP to the GSC. In figure 3, all LDACS entities and protocol stack with their respective communications channels, black for user data and red/blue for radio/sub-net control data, and functionalities as described in the previous section.

3. LDACS's Cybersecurity Architecture

An initial draft for LDACS's cybersecurity architecture was presented in [13] providing protection against previously identified threats (e.g., [12, 27, 28]). In the following an overview of identified asserts, threats, and objectives is presented leading to a more detailed cybersecurity architecture for LDACS and are kept in mind for the performed threat-and-risk analysis.

3.1. Assets, Threats, and Objectives

Anything that someone places value upon is regarded as **asset**. for LDACS five assets were identified: (1) hardware, (2) software, (3) link, (4) data, and (5) services.

LDACS's hardware applied in communication/navigation systems is responsible for the execution of LDACS relevant software, enabling the functionality of LDACS and where LDACS relevant information is stored on. This refers to AS, GS, and GSC but also to an Authentication, Authorization and Accounting (AAA) server, e.g., integrated within the GSC, Access Routers, the links between entities and the respective LDACS specific internal and shared network and routers.

LDACS's software for communication/ navigation capabilities needs to be integrity, authenticity and property proven. Thus we need to make sure that a software component of the devices or sub system is not corrupt, has no errors or other defects. Also we have to prevent wrong installation or configuration of the software components.

All required **data links**, accurate time synchronization along with LDACS control data and radio communications connections enabling LDACS to transmit send and receive data via that link are assets. Most important here is preventing unauthorized access, altered hardware, jamming and spoofing. However, we will not introduce hardware protection mechanisms such as regular quality checks, access limitations to special hardware and control of personal working on that hardware but rather focus on protection of software, the radio link and transmitted data due to the early specified state of LDACS.

Data relevant for an error-free execution of the LDACS communications system needs to fulfill and/or support the following six items:

1. Identity of communication users and entities or participants
2. The actually transmitted or received communication data
3. Confidential data, only accessible for legitimate users and entities only
4. Cryptographic keys used for encryption, decryption, integrity protection and authentication
5. Configuration data to control, configure or alter the functionality and behavior of LDACS
6. Navigation data including cell location and synchronization like the synchronous time in the ground stations

Several services are required for LDACS to properly function. The system management, announcement and routing, mobility and authentication service are needed for general operability of LDACS. As use case, at least 21 high critical user data services in Air Traffic Services (ATS) and 14 high critical Aeronautical Operational Control (AOC) data services [5, 12, 27] will run on application layer. As new functions in ATS and AOC services can be introduced on a frequent basis, this work can only contribute to highlighting already existing safety relevant services in regard to LDACS. Examples of them are the ATC Clearance (ACL), Data Link Logon (DLL), Flight Plan Consistency (FLIPCY), Flight Plan Data (FLTPLAN), Network Connection NETCONN or Network KeepAlive NETKEEP service.

Previous analysis identified a series of cybersecurity **threats** to LDACS [5, 12, 19]. They mainly cover the ares of (1) disclosure of information (2) denial of service and (3) unauthorized entry to system. A selection of example threats is listed in Table 1 and used for comparison reason with [10] and in section 4.2.

Table 1: Selection of security threats to LDACS

Category	Subcategory
Disclosure of Information	(T1) Scanning the Network (T2) Eavesdropping (T3) Man in the Middle attack
Denial of Service	(T4) Flooding (T5) Injecting (T6) Interfering
Unauthorized entry to system	(T7) Altering messages (T8) Impersonation of other participants of communication

The LDACS Standards and Recommended Practices (SARPS) [29] identified among other sources [5, 12, 13] the following **security objectives** for LDACS:

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 non-repudiation 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.

3.2. Architecture Overview

An initial architecture was already presented in [13] and, thus, this section only focuses on the current updates of the LDACS cybersecurity architecture regarding security functions and support.

For secure communication and operation of LDACS we need to support and offer the following:

1. Authentication, Authorization, Accounting (AAA)
2. Availability robustness,
3. Secure key agreement and negotiations,
4. Secure key derivation, key and access management,
5. Confidentiality,
6. Data integrity,
7. Secure logging, and
8. System integrity.

In order to address these eight items a suitable set of algorithms, protocols, and LDACS software are required.

As the initial requirement for the envisioned set is that everything needs to be resource-efficient that is integrated into LDACS. Thus, the essential question to be answered is where to locate the intended security functions in LDACS. The most memorable finding in the placement of the security functions are ideas to rely mostly on the LDACS Management Entity (LME) and Sub-Network Protocol (SNP) layers of the protocol stack for additional cybersecurity in LDACS.

Previous works [5, 28] suggested putting most security functionality in the resource allocation level or the Data Link Service (DLS) fragments. We think that LME and SNP are more suitable due to the following reasons: (1) after being processed by lower layers, the first signal to reach an AS from a GS, arrives at the LME to enable the access to a LDACS cell. (2) Putting additional authentication and negotiation functionalities in that layer produces little overhead and enables a secure link. (3) As for user data, incoming from the network and application layer higher up in the ISO/OSI stack, the first step is to put the payload in sub-network LDACS specific PDUsin the SNP. (4) Also with the information from the network layer, whether encryption should be used or not, this task can directly be executed without the necessity of lower layers to know about it. And (5) finally, it gives our system the advantage to support real end-to-end security as the data packets are secured between the leaving of the ATM system at the inter ace to the GSC and the AS SNP and vice-versa, where security checks can be performed. Also as the DLS supports a checksum, it is guaranteed that packets arriving at the SNP are error free and thus if an integrity check or decryption fails at the SNP, it is highly likely that the data has been tampered with.

LME and SNP communicate via the same primitive with lower layers, making it easy to put additional security in the data channel using the highest fragment/packet priority that is solely reserved for security data. Before a security clearance, data packets with lower priority cannot be transmitted or are dropped.

The identified arguments answering the location question inspired the final implementation in LDACS described in the following.

For AS, GS, and GSC to securely communicate with each other they need to (1) mutually authenticate by using certificates (2) that are linked in a LDACS Public Key Infrastructure (PKI), similar to AeroMACS [9, 10]. As Bradford et al. mentioned in [30], different propositions exist how a PKI might look like for all Future Communications Infrastructure (FCI) candidates (AeroMACS, LDACS, SatCOM) as depicted in figure 5. Currently the most viable solution also suitable for LDACS is the ICAO Trust Bridge as AeroMACS has already started with that approach [10]. Other approaches are to use a regional cross certification meaning, that continents, countries or sectors would need to cross certify their counterparts in different regions of the world, leading to a mesh network of trust. Currently the least likely candidate is a trust list certification, meaning that Certificate Authorities (CA) from different regions have to put trust in each end-entitiy certificate. However the discussion which solution will be finally used is still ongoing.

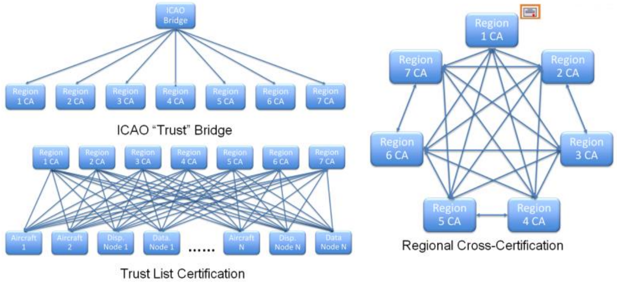

Figure 5: Possibilities on how to establish a Chain-of-Trust for all FCI candidates.

After authentication of the network participants AS, GS, and GSC (depicted in figure 6), key negotiation starts (3) resulting in a key agreement. Next, a key derivation function (KDF) derives sufficiently enough session keys (4) for all sessions and maintaining perfect forward secrecy (PFS). Now the LME hands over the negotiated and derived keys to the DLS (4) and authorizes the entity it has authenticated and negotiated a key with, for commencing secure communications (5). The DLS hands over the keys to the SNP (6), which in turn can start encrypting/decrypting data and apply or verify message authentication codes to the SNP (7). The SN-PDUs consists of a LDACS specific header, payload from the transport layer above (e.g., using the well-known IPv6 and TCP/UDP stack), and a trailer with the message authentication codes attached. With the ability of the SNP to perform those tasks, the DLS can now start processing the SN-PDUs (8).

The MAC layer secures the logical channels (1-8) by allowing signatures to be broadcast from a ground station, thus making the validation of the authenticity of that ground station possible at the first step. Our findings indicate, that while other control channels such as the CCCH, DCCH and RACH simply lack the space for additional security placement, the BCCH offers enough to put a 128 bit overhead here for signing that control message [6]. However CCH, DCCH and RACH are monitored by the MAC for plausibility, such as the avoidance of too many reoccurring messages or resource requests. All actions related to LDACS cybersecurity are logged in the LME. Figure 6 illustrates the aforementioned eight steps answering the location question in the stack of AS/GS.

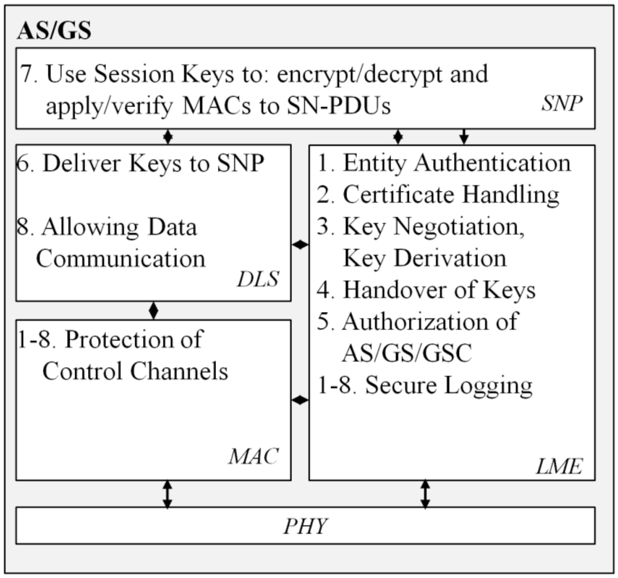
AS/GS
7. Use Session Keys to: encrypt/decrypt and apply/verify MACs to SN-PDUs
SNP
6. Deliver Keys to SNP
8. Allowing Data Communication
DLS
1-8. Protection of Control Channels
MAC
1. Entity Authentication
2. Certificate Handling
3. Key Negotiation, Key Derivation
4. Handover of Keys
5. Authorization of AS/GS/GSC
1-8. Secure Logging
LME
PHY

Figure 6: Steps realizing secure communication

When not having the focus for secure communication establishment on the placement of the functionalities in the stack, the complete process can be broken down into three phases depicted in Figure 7:

- Phase 1: GSC and GS establish a secure connection using e.g., the Station-to-Station protocol, as suggested below. This allows for mutual authentication and key negotiations. After mutual authentication, a key confirmation message concludes this phase.
- Phase 2: Now GSC and GS have established a trusted connection and the GS can start broadcasting beacons in the BCCH with parameters provided by the most

trusted entity, the GSC. This allows for incoming AS to identify and authenticate the GS on first contact. If the AS has verified the identity of the GS, a cell entry request can be sent from the AS, as it is now assured to be talking to a legitimate GS.

- Phase 3: The AS can send its credentials to the GS as it has established an untrusted connection with the GS after cell entry. Now GS and GSC can verify the claimed identity of the AS and after authentication of the AS, mutual key negotiations can start, resulting in derived session keys and a key confirmation message between GSC and AS. Thus we have established a secure connection between AS and GSC.

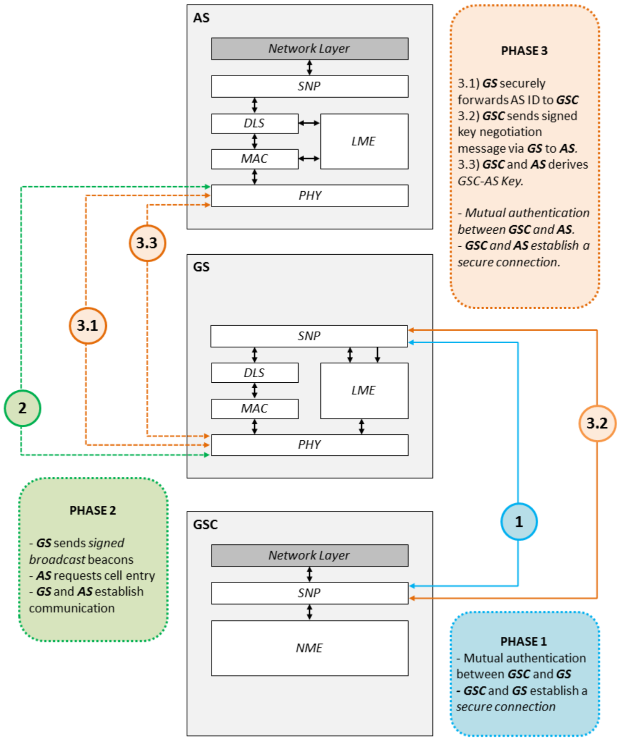
AS
Network Layer
SNP
DLS
MAC
LME
PHY
GS
SNP
DLS
MAC
LME
PHY
GSC
Network Layer
SNP
NME
3.3
3.1
2
3.2
1
PHASE 3
3.1) GS securely forwards AS ID to GSC
3.2) GSC sends signed key negotiation message via GS to AS.
3.3) GSC and AS derives GSC-AS Key.
- Mutual authentication between GSC and AS.
- GSC and AS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

Figure 7: Phase concept to establish secure communication [13]

As soon as a secure communication possibility is in place the data exchange can happen.

3.3 Protocol Selection for strengthening LDACS Cybersecurity Architecture

Here we point out which algorithms and protocols should be used, fulfilling the request of resource-efficiency and the eight security requirements mentioned in the beginning of Section 3.2. After several months of investigation and analysis of different approaches we received the following recommendation list:

1. Trust comes via distributing trust from offline-ICAO CA, Sub-Ca, until end-entity certificate in the end device. We suggest X.509 certificates and distribution of them in a chain of trust. However as quantum computers with sufficient Q-Bits do not seem far off, RSA asymmetrical procedures can only be used in the short term due to Shor's algorithm [31]. To replace that we would recommend a key-size optimized McEliece post-quantum robust procedure [32].

2. Entities must be mutually authenticated, where we recommend the Station-to-Station protocol due to low overhead and key agreeing possibilities [33].

3. To negotiate key material between entities we also recommend the Station-To-Station protocol with the same reasons as before.

4. To derive arbitrary number of keys we recommend using a HMAC-Key Derivation Function (HKDF) such as defined in RFC 5869 [34].

5. As entities need to be loosely time synchronized, we can use the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) broadcast authentication protocol [35] for securing our broadcast beacons rom the GS.

6. For encryption we recommend AES-256-GCM with Galois Counter Mode (GCM) being a mode of operation on symmetric key block. It provides authenticated encryption/decryption and can also be used for integrity protection [36].

7. In terms of integrity and authenticity of messages in transit, we recommend HMAC with trapdoor functions from the SHA-3 family [37, 38] or as mentioned above, AES-GCM.

4. Threat-and-Risk Analysis

Already in [12] LDACS was rated. The main outcome here was that no cybersecurity was implemented then and thus all threats were dangerous for LDACS. With the updates and the security improvements introduced throughout the earlier sections of this paper we can state that the cybersecurity support is now strengthened in LDACS. In order to prove this, a threat-and-risk analysis is performed here. But keep the following in mind: By identifying threats impacting confidentiality, integrity or availability we set out a collection of threats to test LDACS robustness, with and without our proposed security architecture. This threat catalogue is not complete but spans a rather broad scope of possible attacks. We chose a limited threat catalogue, already shown in Table 1, with exactly the chosen threats to be able to measure LDACS robustness against various attacks, but also to not overcomplicated threat identification as there are an unlimited numbers of possible threats to LDACS.

4.1. Methodology

The rating methodology applied here is similar to the one already performed in [12], however now on the LDACS system with security additions. We chose the Common Criteria (CC) process also for the rating procedure, with averaged likelihood and maximum severity, as the CC methodology is also a guide for the evaluation IT products with security functionality [36].We adapted previous quantitative threat rating scales to give a quantitative measurement of the risk a certain threat poses. A severity-likelihood matrix is commonly used to rate a certain threat [36] but the method on how to weight severity and likelihood can differ

We decided to take the severity rating as done in the Communications Operating Concepts and Requirements (COCR) analysis [19] but for likelihood, we defined our own solution introducing the following factors [12]:

- Elapsed Time
  Time required identifying a vulnerability, to develop an attack and to mount and sustain it.
- Expertise
  We set the scale from no technical knowledge required to several experts from different fields required to successfully launch an attack.
- Knowledge of System
  Here we rate from “public knowledge” to “highly confidential”.
- Window of Opportunity
  We describe this as the time we need for the system to be accessible for successfully attack it.
- Equipment
  This measures the quality of equipment needed for an attack, from highly available to multiple bespoke specialized hard- and software.
- Distributed Attack
  In order to launch a successful attack, how many targets needs to be compromised, is measured here from one to more than 100 different targets.
- Location dependent
  Accessibility of an online or offline only target defines part of the difficulty for attacking it.

Each factor was rated from 0 to 5 based on a defined premise with 0 being the most likely event and 5 the least likely. The average value of these factors was finally set as the likelihood of a threat to occur with a value of 0 - 1 being “very likely" and 4 - 5 being “extremely improbable".

Introducing a quantitative threat rating system for a non-operational system is challenging, as we need quantifiable values for that like amounts of vulnerabilities, severity of vulnerability, etc.. And as we do not have that, the values used for the severity-likelihood matrix emerge entirely from reasoned evaluation of the threats danger by a Cybersecurity expert. Also, our threat-and-risk analysis revealed, that prior to [4, 12, 28] and this work, basically no cybersecurity measures were implemented in LDACS, making it very vulnerable in its state, prior to our architecture proposal.

4.2. Comparing LDACS Security Level with and without the Security Additions

In our rating system, there are three levels:

”Negligible” (Green) meaning the threat is known and accepted, but deemed harmless.

“Medium” (Yellow) meaning that no immediate actions, e.g., additional encryption, software patches, must be done to hinder the occurrence of the threat, but the threat itself and its development will be looked at closely.

“Dangerous” (Red) indicates that the impact of a successful attack is not acceptable and direct counter measures (e.g., changing cipher suite, updating system) must be introduced.

Before the deployment of the LDACS's cybersecurity architecture three of the eight threats were rated as medium and five as dangerous (cf. Table 2). Now we do the same evaluation with the security measures included in the LDACS protocol stack specified in Section 3.2 and illustrated in Figure 5.

Threat #1 - Scanning the Network:

This threat was previously rated as medium because gaining access to the LDACS network and sending probes is easier when no encryption, entity authentication or integrity checks for messages is deployed. Now with added access protection mechanisms, we have hardened LDACS against this threat. We now rate it as negligible.

Threat #2 – Eavesdropping:

Without encryption, listening on the same frequency enabled capturing the ATN data stream from aircraft to ground station, which is why we rated it as dangerous. With the added encryption of Aeronautical Operational Control (AOC) traffic, capturing data became harder. However to entirely protect all ATM traffic, the relevant flight surveillance companies, such as EUROCONTROL, must have access to the decryption keys of all Air Traffic Services (ATS) streams from all flight surveillance authorities. ATS is regulating and assisting aircraft in real-time for ensuring their safe operations, thus higher latency, introduced by the key-sharing and decryption process, introduces an additional safety risk. With these results we prevent eavesdropping on just a part of the data exchange, with the need of organizational changes in the field to enable the entire encryption of ATM traffic. Thus, the threat still remains dangerous and countermeasures must be investigated and integrated as soon as possible.

Threat #3 - Man in the Middle Attack:

With no entity authentication, just inserting another party into the communication and reading the traffic is possible. However if the intercepted packets were to be altered and reinserted to the system, the attacker had to make sure that the original packets would not reach the recipient, which is a very hard task in wireless communications. As a successful Man-in-the-Middle (MITM) attack has a very high impact on the system in total and as there were no counter measures against this attack, we gave this attack the rating dangerous. Now as every participating entity has to authenticate to each other and integrity checks are applied to the messages, becoming a man in the middle proves a harder task than before. Thus, we rate it now as medium.

Threat #4 - Flooding the network:

Unfortunately our cybersecurity architecture update did not include any direct flooding prevention mechanisms except for rate limiting from certain entities. But as rate limiting, load mitigation and rerouting can be enough against flooding attacks, we reduce the threat level from dangerous to medium.

Threat #5 - Injecting messages:

Injecting messages to a system is easier when the participants do not need to authenticate to each other. With the introduction of entity authentication and integrity checks, we hardened LDACS against this threat. Now an entity can still send in the LDACS cell because of its wireless nature, but packets from unauthenticated source will be dropped. The rating itself still remains medium, but loses one point in likelihood as performing such an attack is now more difficult.

Threat #6 - Interfering with the data link:

Jammers, physical violence against LDACS hardware or power outages are not regarded in the architecture thus the threat rating remains medium.

Threat #7 - Altering messages:

Previously rated as dangerous, the risk of this threat has been reduced by several means. Entity authentication prevents easy access to the system, encryption prevents reading of actual messages but ultimately integrity checks in the form of message authentication codes attached to messages can harden against this threat. Thus we rate it as medium now.

Threat #8 - Impersonating other participants of communication:

Before additional measures, this threat was rated dangerous. Now the impersonation is much harder, as access to private keys of legitimate communication participants would be required due to the entity authentication mechanism. Or the cryptography behind our concept would have to be broken.

4.2.1 LDACS without Security Additions

For comparability reasons with the new rating of LDACS' cybersecurity, we provide the old rating from [12] in table 2, where we see that the majority of threats #2, 3, 4, 7, 8 were rated dangerous.

Table 2: Threat criticality rating on LDACS without its cybersecurity architecture

Severity/Likelihood	1 - None	2 - Minor	3 – Major	4 - Hazardous	5 - Catastrophic
1 – Very Likely	🟩	🟨	🟥	🟥	🟥
2 – Probable	🟩	🟨	Threat 1	Threat 4	🟥
3 – Remote	🟩	🟩	🟨	Threats 2,3,7,8	🟥
4 – Very Remote	🟩	🟩	🟨	Threats 5,6	🟥
5 – Extremely Improbable	🟩	🟩	🟩	🟩	🟨

4.2.2 LDACS with Security Additions

As we have described the changes in cybersecurity due to the introduction of our cybersecurity solution for LDACS in chapter 4.2, we sum up the rating of severity in table 3. Values in **bold** are the final rating, derived from taking the maximum value from all rows in a column.

Table 3: Threat severity rating

Properties	Threats							
	T1	T2	T3	T4	T5	T6	T7	T8
Availability of flight routine	1	1	1	**3**	2	2	2	3
Air Traffic Control	**2**	1	2	**3**	2	**4**	**3**	3
Cost	1	3	2	**3**	2	3	2	2
Fatalities	1	1	1	1	1	3	1	1
"Flying Public"	1	1	2	**3**	2	3	2	2
Exposure of proprietary information	**2**	**4**	**4**	1	**3**	1	2	**4**
Maximum	**2**	**4**	**4**	**3**	**3**	**4**	**3**	**4**

For likelihood, we take the following formula: $\left\lfloor \frac{\sum Factor}{|Factors|} \right\rfloor$, thus we take the average value of all rating factors and use the floor function. The result is depicted in table 4:

Table 4: Threat likelihood rating

Factor	Threats							
	T1	T2	T3	T4	T5	T6	T7	T8
Elapsed Time	3	3	4	3	4	3	4	4
Expertise	3	3	4	3	4	4	4	4
Knowledge of System	3	3	4	3	4	4	4	4
Window of Opportunity	1	3	3	1	3	2	3	4
Equipment	1	2	2	1	3	4	3	2
Distributed Attack	3	4	3	2	3	3	3	2
Location dependent	3	2	3	2	3	4	3	3
Average	**2.4**	**2.9**	**3.3**	**2.1**	**3.4**	**3.4**	**3.4**	**3.3**
Rating	**3**	**3**	**4**	**3**	**4**	**4**	**4**	**4**

Finally we use our values from severity and likelihood and put it into our severity, likelihood matrix from the common criteria process [12, 36].

As we can see in table 5, the impact of threats was reduced significantly, when comparing to LDACS previous state. Only one threat remained as dangerous, simply because there will be unencrypted traffic in the system, easy to eavesdrop upon.

Table 5: Applying the rating system onto selected threats to LDACS with cybersecurity additions

Severity/Likelihood	1 - None	2 - Minor	3 – Major	4 - Hazardous	5 - Catastrophic
1 – Very Likely	🟩	🟨	🟥	🟥	🟥
2 – Probable	🟩	🟨	🟨	🟥	🟥
3 – Remote	🟩	Threat 1	Threat 4	Threat 2	🟥
4 – Very Remote	🟩	🟩	Threats 5,7	Threats 3,6,8	🟥
5 – Extremely Improbable	🟩	🟩	🟩	🟩	🟨

5. Conclusion

In this paper an updated LDACS architecture was introduced with focus on cyber security support. It was clearly justified where which security function should be placed in the stack to be resource-efficient and allowing simple interaction with the components of DLR’s “Networking the Sky” concept. Especially, the direct comparison concerning threat rating showed that with the integration of security functionality in LDACS threats’ impact could be reduced. Only the risk of jamming the wireless communication could not be diminished which is challenging in general and is still under investigation in many disciplines.

Based on the received results security functionalities need to be included in the standardization process of LDACS in order to face crime activities. We are convinced that with our contributions, LDACS will have a better chance at being deployed worldwide as the standard for civil aeronautical communications in the continental areas for the next thirty years to come.

References

[1] EUROCONTROL, "EUROCONTROL’s Challenges of Growth 2018 Study Report", EUROCONTROL, 2018. [Online]. Available: https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/reports/challenges-of-growth-2018.pdf. [Accessed 20.02.2019].

[2] T. Keaveney and C. Stewart, "Single European Sky ATM Research Joint Undertaking", SESAR , 2019. [Online]. Available: https://www.sesarju.eu/. [Accessed 19.02.2019].

[3] U.S. Department of Transportation Federal Aviation Administration, "Next Generation Air Transportation System", FAA, 2019. [Online]. Available: https://www.faa.gov/nextgen/. [Accessed 19.02.2019].

[4] A. Bilzhause, B. Belgacem, M. Mostafa and T. Gräupl, "Datalink security in the L-band digital aeronautical communications system (LDACS) for air traffic management", IEEE Aerospace and Electronic Systems Magazine, 32(11), 22-33, Nov 2017.

[5] M. Mahmoud, A.Pirovano and N. Larrieu, "Aeronautical communication transition from analog to digital data: A network security survey", Computer Science Review, 11:1-29, 2014.

[6] T. Gräupl. C. Rihacek and B. Haindl, "LDACS A/G Specification", German Aerospace Center (DLR), Germany, SESAR2020 PJ14-02-01 D3.3.010, 2017.

[7] T. Gräupl and M. Ehammer, "L-DACS1 Data Link Layer Evolution of "ATN/IPS", 30th Digital Avionics Systems Conference (DASC) Proceedings, October 16-20, 2011, Seattle, Washington, USA, 2011.

[8] T. Gräupl, M. Ehammer and C.H. Rokitansky, "Simulation Results and Assessment of the NEWSKY Concept for Integrated IP-Based Aeronautical Networking", 28th Digital Avionics Systems Conference Proceedings, 25-29 October, 2009, Orlando, FL, 2009.

[9] S. Wilson, "The network security architecture and possible safety benefits of the AeroMACS network", Integrated Communications, Navigation and Surveillance Conference (ICNS) Proceedings, May 10-12, 2011, Washington DC, USA, IEEE, 2011.

[10] B. Crowe, "Proposed AeroMACS PKI Specification is a Model for Global and National Aeronautical PKI Deployments", WiMAX Forum, Integrated Communications Navigation and Surveillance Conference (ICNS) Proceedings, April 19-21, 2016, Washington DC, USA, IEEE, 2016.

[11] M. Bartock, J. Cichonski and J. Franklin. "LTE Security–How Good Is It?", National Institute of Standards & Technology (NIST), US Department of Commerce, Gaithersburg, MD, USA, Tech. Rep 3, 2015.

[12] N. Mäurer and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis", Integrated Communications, Navigation and Surveillance Conference (ICNS) Proceedings, April 10-12, 2018, Washington DC, USA, IEEE, 2018.

[13] N. Mäurer and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)", 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC) Proceedings, September 23-27, 2018, London, England, IEEE, 2018.

[14] D. M. Mielke, "C-band digital aeronautical communication for unmanned aircraft systems", IEEE/AIAA 36th Digital Avionics Systems Conference (DASC) Proceedings, 17-21 September, 2017, St. Petersburg, Florida, USA, IEEE, 2017.

[16] T. Gräupl and M. Ehammer, "Simulation Results and Final Recommendations of the SANDRA Concept for Integrated IP-Based Aeronautical Networking", Integrated Communications Navigation and Surveillance (ICNS) Conference Proceedings, 22-25 April, 2013 Herndon, VA, 2013.

[17] S. Brandes, S. Gligorevic, M. Schnell, C.H. Rokitansky, M. Ehammer, T. Gräupl, A. Schlereth, and C. Rihacek, "Final Assessment of the B-VHF Overlay Concept", IEEE Aerospace Conference Proceedings, 3-10 March, 2007, Big Sky, MT, 2007.

[18] M. A. Bellido-Manganell, T. Gräupl and M. Schnell, "Impact Assessment of the L-Band Digital Aeronautical Communications System on the Joint Tactical Information Distribution System", IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2019.2898524, 2019.

[19] EUROCONTROL, FAA, and Future Communications Study Operational Concepts and Requirements Team, "Communications Operating Concept and Requirements for the Future Radio System (COCR)", EUROCONTROL/FAA, 2007.

[20] T. Gräupl, M. Ehammer, E. Pschernig, C. Rokitansky, C. Morlet, L. Albiol Schnitger and Paolo Conforto, "Dimensioning Requirements for the ANTARES ATM Satellite Data-Link", Integrated Communications Navigation and Surveillance Conference (ICNS) Proceedings, May 11-13, 2010, Herndon, VA, 2010.

[21] S. Plass, R. Hermenier, O. Lücke, D. Gomez Depoorter, T. Tordjman, M. Chatterton, M. Amirfeiz, S. Scotti, Y. J. Cheng, P. Pillai, T. Gräupl, F. Durand, K. Murphy, A. Marriott and A. Zaytsev, "Flight Trial Demonstration of Seamless Aeronautical Networking", IEEE Communications Magazine, vol. 52, no. 5, May 2014.

[22] M. Schnell, U. Epple, D. Shutin and N. Schneckenburger, "LDACS: Future aeronautical communications for air-traffic management", IEEE Communications Magazine, 52(5):104-110, 2014.

[23] O. Marcia, "AeroMACS PKI", Integrated Communications, Navigation and Surveillance Conference (ICNS) Proceedings, April 10-12, 2018, Washington DC, USA, 2018.

[24] M. Ehammer and T. Gräupl, “AeroMACS – An Airport Communications System”, 30th Digital Avionics Systems Conference Proceedings, 16 - 20 October, 2011, Seattle, WA, 2011.

[25] C. Morlet, M. Ehammer, T. Gräupl and C.H. Rokitansky, "Characterisation of the Data Link Communication Air Traffic for the European Airspace", 29th Digital Avionics Systems Conference Proceedings, October 3-7, 2010, Salt Lake City, UT, 2010.

[26] T. Gräupl, M. Ehammer and C.H. Rokitansky, "Link-Layer Quality of Service in the L-Band Digital Communication System B-AMC", 27th Digital Avionics Systems Conference Proceedings, 26-30 October, 2008, St. Paul, MN, 2008.

[27] N. Zelkin and S. Henriksen, "L-band digital aeronautical communications system engineering - initial safety and security risk assessment and mitigation", ITT Corporation Advanced Engineering & Sciences Division, Herndon, Virginia, NASA, 2011.

[28] R. Wernsdorf, J. Posegga, S. Huber, A. Bilzhause and D. Sörgel. "L-DACS1: Assets, Protection Requirements, Threat Analysis and Security Objectives", Technical report, Nationales Luftfahrtforschungsprogramm, Vierter Programmaufruf (2012 to 2015), BMWT, GERMANY, 2014.

[29] C. Rihacek, B. Haindl, P. Fantappie, S. Pieratelli, T. Gräupl, M. Schnell and N. Fistas, „L-band Digital Aeronautical Communications System (LDACS) activities in SESAR2020", Integrated Communications, Navigation and Surveillance Conference (ICNS) Proceedings, April 10-12, 2018, Washington DC, USA, 2018.

[30] S. Bradford, "Cybersecurity for global Aviation - A Trust Framework enabling global secure aviation interoperability", FAA, Integrated Communications, Navigation and Surveillance Conference (ICNS) Proceedings, April 10-12, 2018, Washington DC, USA, 2018.

[31] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a

quantum computer", SIAM review 41.2 303-332, 1999.

[32] H. Bartz and G. Liva, "On decoding schemes for the MDPC-McEliece cryptosystem", arXiv preprint arXiv:1801.05659, January, 2018.

[33] S. Blake-Wilson and A. Menezes, "Unknown key-share attacks on the station-to-station (STS) protocol", International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, 1999.

[34] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5869. [Accessed 17.01.2019].

[35] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "The TESLA broadcast authentication protocol", Rsa Cryptobytes, 5(2), 2-13, 2005.

[36] U.S. Department of Commerce - Acting Secretary R. M. Blank, "Security and Privacy Controls for Federal Information Systemsand Organizations", NIST Special Publication 800-53 Revision 4, 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed 10.01.2019].

[37] M. Bellare and B. Tackmann, "The multi-user security of authenticated encryption: AES-GCM in TLS 1.3", Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 2016.

[38] M. M. Mathews and V. Panchami, "Date time keyed-HMAC", 2016 Online International Conference on Green Engineering and Technologies (IC-GET), IEEE, 2016.

Email Addresses

nils.maeurer@dlr.de

corinna.schmitt@unibw.de