PAVING THE WAY FOR AN IT SECURITY ARCHITECTURE FOR LDACS: A DATALINK SECURITY THREAT AND RISK ANALYSIS

Nils Mäurer, German Aerospace Center, Oberpfaffenhofen, Germany
Arne Bilzhause, Universität Passau, Passau, Germany

Abstract

With air transportation growing and current civil aeronautical communication systems reaching their capacity limit in high density areas, the need for new aeronautical communication technologies becomes apparent. This implies the transition from analogue voice to digital data communication. A promising candidate for terrestrial air-ground communication is the L-band Digital Aeronautical Communications System (LDACS). LDACS is currently in the process of being standardized in ICAO. Being integrated in the aeronautical telecommunication network and providing a digital communication link for safety critical applications, each and every installation of LDACS requires protection against cyber-attacks. A rigorous threat and risk analysis is the fundamental basis to derive an IT security architecture for LDACS. The objective of this paper is to identify safety relevant air traffic management services, perform a threat and risk analysis, and define attacker types. Having created a threat catalog, we introduce a threat rating system allowing us to set our findings in a qualitative context and pave the way for a future LDACS IT security architecture.

Introduction

Developing new means of communication for future aeronautical communications is one of the major tasks for civil aviation in the years to come [1].The necessity for new aeronautical communications becomes apparent when having a look at estimates of the increase in number of flights worldwide, stating that there will be a growth of 50% more flight movements in 2035 compared to 2012 [1]. Thus the current Air Traffic Management (ATM) system, in particular in Europe and the US, will reach its current capacity limit [2]. Analogue systems have therefore to be replaced by digital means and the entire aeronautical communications of tomorrow will likely be running on an IP-based architecture [3]. The L-band Digital Aeronautical Communications System (LDACS) is a candidate for future air-to-ground communications that has been developed in cooperation between the German Aerospace Center (DLR) [2], Frequentis AG [4], and the University of Salzburg in Austria [5, 6]. With the change from analogue to digital wireless communications, LDACS requires a thorough IT security analysis in order to protect the system properly against threats from the IT sector [7]. Project ICONAV[1] was a first attempt to perform this analysis and to develop a "base line protection" security architecture for LDACS that was not yet comprehensive [8]. However, a comprehensive and well-designed security concept for LDACS is key to its deployment and success.

The main contribution of this paper is an extensive threat and risk analysis of LDACS and the introduction of a threat rating system allowing us to set our findings in a qualitative context. Based on that outcome, we can define IT security objectives and functions, allowing us to lay the foundation for future security mechanisms to protect LDACS against adversaries.

Background

At the eleventh ICAO air navigation conference in 2003, the necessity for evolution of the aeronautical air-ground communication became apparent [9]. The transition to a future air-ground communication infrastructure was identified as a prerequisite to provide the capacity required to handle future air traffic management data traffic.

To identify relevant features and to evaluate whether an already existing system can meet the requirements for the future communications infrastructure the Federal Aviation Administration (FAA) and EUROCONTROL started a joint study called Action Plan 17 (AP17). The outcome was that no single technology can fulfil all demands [10].AP17 sparked therefore the development of new

[1] http://www.dlr.de/kn/desktopdefault.aspx/tabid-4309/3222_read-36946/admin-1/

978-1-5386-5679-2/18/$31.00 ©2018 IEEE

systems based on the identified necessities and desired features. For the en-route domain LDACS is the designated system, with its origins in merging parts of the B-VHF [11], B-AMC [12, 13, 14], TIA-902 (P34), and WiMAX IEEE 802.16e technologies [15].

Threat and Risk Analysis

Methodology

The approach used in this paper is based on established standards. Guidelines for threat and risk analysis of IT security flaws and errors in technical systems are published in ISO norm 27001, IEC norm 62443, and the Common Criteria for Information Technology Security Evaluations (CCfITSE) [16, 17, 18]. We chose these norms, and especially the Common Criteria (CC) process as they are designed to be "useful as a guide for the development, evaluation and/or procurement of IT products with security functionality" [16]. However, we do not follow the entire CC process yet as LDACS is still in development and changes are still being made in the standard [6]. This approach still suffices to provide orientation in the design process of IT security measures.

In additions to the available standards, several works provide guidelines, case studies, and preliminary work on LDACS. Mahmoud et al. [19] provide a full example on how to conduct a threat and risk analysis on a technical system based on a quantitative approach making the results measurable and not dependent on the expertise of single IT security authorities in the field. With AeroMACS having its origin in WiMAX, its security features are similar and are described in [20]. Tamasi et al. [21] provide real life examples and analysis chains on how to rate findings. This was later continued by Schäfer et al. [22] who provide more recent examples. Bilzhause et al. [8] analyzed possible implementation options of IT security in LDACS.

Assets

Based on the analysis of security objectives in the field of communications system in civil aviation [20, 23] we had a closer look on the procedure followed in identifying assets and security objectives in LDACS. The term asset is hereby defined as an entity that the owner of a system places value upon [10]. We start by looking at the three most important business goals for information security of the Future Communications Infrastructure (FCI) according to COCR [23]:

Safety: The FCI must sufficiently mitigate attacks, which contributes to safety hazards.

Regularity of flight: The FCI must sufficiently mitigate attacks, which contribute to delays, diversions, or cancellations to flights.

Protection of business interests: The FCI must sufficiently mitigate attacks which result in financial loss, reputation damage, disclosure of sensitive proprietary information, or disclosure of personal information.

Projecting these goals on the LDACS subsystem leads to the following categorization:

Asset – Hardware: The LDACS hardware applied in communication/navigation systems, responsible for the execution of LDACS relevant software, enabling the functionality of LDACS and where LDACS relevant information is stored on.

Asset – Software: The software applied in LDACS communication/navigation and also the intellectual and physical ownership of that software.

Asset – Link: All required data links and radio communications connections enabling LDACS to transmit and receive data via that link.

Asset – Data: We list all required data relevant for an error-free execution of the LDACS communications system as follows:

1. Identity of entities participating in the communication
2. The actually transmitted or received communication data
3. Confidential data, only accessible for authorized legitimate entities (this is nonexclusive with other items of the list)
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

Safety Relevant Services

When investigating the possible services supported by LDACS, it is important to note that in general there are five different types of services [3, 17, 20]: (1) Voice over Very High Frequency (VHF) is the basic dialogue mode when performing air traffic control operations. (2) Air Traffic Services (ATS) serve flight management and include communication related to the safety and regularity of the flight. It is used for air-to-ground or air-to-air communication. (3) Aeronautical Operational Control (AOC) is mainly dedicated to flight operation and maintenance. (4) Aeronautical Administrative Communications (AAC) serve business operations of the airline like cabin-management and in-flight passenger service. (5) Aeronautical Passengers Communications (APC) are dedicated to passenger communications inside the cabin.

Additionally the Network Management (NM), even though not mentioned as an explicit separate service, is important to be able to transmit any data at all. Thus, there are six different basic services. In this work we will focus on the data link of the communications technology LDACS which aims to meet safety and regularity of flight communications requirements, in particular those supporting air traffic services and safety related aeronautical operational control communications. To provide these services, a stable and secure network connection is required, thus leaving us with three basic IT security relevant services for our threat and risk analysis: Air traffic services, aeronautical operational control and network management services.

Air Traffic Services

In total we identified 31 air traffic services relevant for LDACS. However, as not all of these services prove safety relevant, we restrict our analysis to those that are. Aligned with analysis from NASA [24, 25] we identified a list of 14 safety related ATS services, which LDACS will support.

ATC (Air Traffic Control) Clearances – ACL: As the ACL exists for clearances for an aircraft's physical location, the danger of wrong positioning or the wrong sector association of an aircraft endangers the physical integrity of the plane.

Common Trajectory Coordination – COTRAC: Used for establishing and coordinating trajectory agreements in real-time using the Flight Management System (FMS), bad positioning in latitude, longitude, altitude, and airspeed is again a danger to the planes physical integrity.

Data Link ATIS (Automatic Terminal Information Service) - D-ATIS: D-ATIS provides automatic assistance in requesting and delivering air traffic information such as meteorological conditions. With a forgery of this information, non-optimal or dangerous flight routes could be chosen by the FMS.

Data Link Logon – DLL: The most important task of the DLL is to uniquely identify an aircraft, thus forgery of these information can lead to disarray in the communication and air traffic management system.

Data link Operational En Route Information Service - D-ORIS: Data for the to be over-flown area is fetched from the D-ORIS service. With missing or forged information the flight routine is endangered.

Data Link Operational Terminal Information Service - D-OTIS: Flight information in the departure, approach or landing phase is provided by D-OTIS. As these are rated as the most critical phases of a flight, wrong or missing information can prove fatal for passengers, the airport or the planes physical integrity.

Data Link Runway Visual Range - D-RVR: When the actual viewing or weather conditions are very poor at an airport, another one might be picked for landing. Disabling the D-RVR or forging information can put a plane in a dangerous situation when the actual conditions do not meet the transmitted ones.

Downstream Clearance – DSC: As with different phases of the flight, different air traffic service units are responsible for that flight and for a transition from one to the other a clearance is required via the DSC. Disabling the DSC would consequently lead to a disruption in the communication.

Data link surface information guidance - D-SIG: False information such as the positioning of other planes or entities of an airport threatens the physical integrity of the aircraft and ground based units.

Data Link Significant Meteorological Information - D-SIGMET: D-SIGMET informs about weather phenomena that may endanger the safety of aircraft operations. Disabling it or inserting falsified information endangers the flight routine and the planes physical integrity.

Flight Plan Consistency – FLIPCY: This service is for detecting inconsistencies between the ATC flight plan and the flight plan activated in the plane's FMS. Without this service, inconsistencies may not be noted and addressed.

Flight Path Intent – FLIPINT: As the name of the service indicates, the chosen trajectory of a plane is synchronized with the responsible air traffic management unit, ensuring the consensus about routes on ground and airborne.

Paired Approach ACL - PAIRAPP ACL: When several aircraft are approaching the same sector, the surveillance and flight intent of all relevant aircraft are exchanged and clearances given by the PAIRAPP ACL preventing in-air close fly-bys or collisions.

Wake Broadcast – WAKE: WAKE keeps planes at a defined minimal distance and works as a safety backup. Disabling it would be one step when trying to manipulate aircraft to collide with each other.

Airline Operational Communications

Continuing with the AOC services, there are a total of 21 services relevant for LDACS, whereas only four have been identified to be safety relevant, again aligned with [23, 24, 25]. To start sending messages and conducting the flight, an indication to the AOC is required, stating that the flight crew has arrived on board. This is done by the AOC Data Link Logon (AOCDLL). The flight plan has to be prepared in accordance with AOC and loaded into avionics, which is done by the FLTPLAN service. Planned load sheet and cargo documentation is provided by the LOADSHT service. In case information is forged or missing, a disparately loaded aircraft can be the consequence of this, rendering it unable to take-off or maintain its center of gravity. The Notice to Airmen (NOTAM) service alerts the flight crew of special events such as military exercises with resulting airspace restrictions. Disabling this can lead to the intrusion of restricted areas and render the planes unable to react to unexpected events.

Network Management Services

Concluding with the network management services, there is the NETCONN which is established between each pair of aircraft and ground systems before ATS or AOC data can be exchanged. It is normally maintained for the entire length of the flight and is vitally important for transferring data, as without the data link no communication can take place. The second service is the NETKEEP, which starts once a connection is established by exchanging network keep-alive messages between the aircraft and ground systems when there is no communication for a period of time, to maintain the status of the connection. Again, this service plays an important role as by altering or disabling NETKEEP, established connections can break down and communication is interrupted.

Summarizing this section, there are a total of 14 ATS, four AOC and two NM services which are safety relevant when running on an underlying LDACS system.

Threat Catalogue

We analyzed how the LDACS subsystem and the identified safety relevant services might be threatened. We started by having an overall look on protection goals of IT security, used in the Common Criteria evaluation process [17]. We define confidentiality, integrity, availability, authenticity and non-repudiation as in [24, 25, 26].

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

System Integrity: Assurance that an information system is operating without unauthorized modification, alteration, impairment, or destruction of any of its components.

Data Integrity: The property that data has not been altered or destroyed without being authorized to do so.

Availability: Assurance that information and communications services will be ready for use when expected.

Authenticity: Property that ensures that the identity of a subject or resource is the one claimed by it.

Non-Repudiation: Ability to prove the occurrence of a claimed event or action and link it evidently to its originating entity.

Analyzing these security goals in the context of LDACS, we identified and selected eight threats displayed in Table 1 in alignment with [16, 24]:

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

Threat Rating System

Now we measure the severity and likelihood of each threat based on the current LDACS specification [4]. To introduce a methodology to rate threats, we decided on a severity versus likelihood matrix to measure the impact and the probability of a threat to actually happen. For that reason we needed to define the properties of likelihood and severity.

Likelihood

From [7] we adopted the concept that likelihood of an actual attack consists of motivation of the attacker and technical difficulty to perform the attack. Thus, the following holds true: The higher the motivation and the lower the difficulty, the higher the possibility of an attack. The opposite also holds. The fundamental problem with this way of defining likelihood is the different existing view points and measurement methods:

- Quantitative - based on measurable numbers
- Qualitative - based on properties and expert judgement how likely an attack is to be conducted

For a quantitative measurement, COCR together with [27] provided numbers of occurrences of incidents within a defined time span in the National Airspace System (NAS) (Table 2). However, there are no publicly available numbers of incidents in the Air Traffic Network (ATN) per operational hour, thus we required another method.

Table 2. Quantitative Measurement of Likelihood of Attacks from the IT Sector on the NAS of the United States of America

Likelihood Class	Amount of Occurrences in the NAS
1 - Extremely Improbable	Probability of Occurrence per operation/operational hour: $<10^{-9}$
2 - Very Remote	Probability of Occurrence per operation/operational hour: $<10^{-7}$ and $>10^{-9}$
3 - Remote	Probability of Occurrence per operation/operational hour: $<10^{-5}$ and $>10^{-7}$
4 - Probable	Probability of Occurrence per operation/operational hour: $<10^{-3}$ and $>10^{-5}$
5 - Very Likely	Probability of Occurrence per operation/operational hour: $>10^{-3}$

Regarding qualitative measurement methods, there are many examples in literature [28, 29] on how to do it .We decided to mix approaches, develop a new and more fine-grained rating system and apply that onto our threat catalogue. For that purpose we defined seven factors all connected to either motivation or technical difficulty and rate them from zero to five (Table 3), average the score and receive a likelihood rating for a certain attack. The final rating is based on the following five categories: *(1) Extremely Improbable* with an average score between 4 and 5, *(2) Very Remote* with an average score between 3 and 4, *(3) Remote* with an average score between 2 and 3, *(4) Probable* with an average score between 1 and 2 and *(5) Very Likely* with an average score between 0 and 1.

Table 3. Qualitative Measurement of Likelihood of Attacks from the IT Sector on the NAS

Factor	Level	Value
Elapsed Time	<= 1 day	0
	<= 1 week	1
	<= 1 month	2
	<= 3 months	3
	<= 6 months	4
	> 6 months	5
Expertise	Computer agnostic	0
	Script Kiddie	1
	Layman	2
	Proficient	3
	Expert	4
	Multiple Experts	5
Knowledge of System	Open	0
	Public	1
	Restricted	2
	Sensitive	3
	Confidential	4
	Critical	5
Window of Opportunity	Unlimited	0
	Very Easy	1
	Easy	2
	Moderate	3
	Difficult	4
	Very Difficult	5
Equipment	Directly available	0
	Standard	1
	Sophisticated	2
	Specialized	3
	Bespoke	4
	Multiple bespoke	5
Distributed Attack	None	0
	Weakly distributed	1
	Minorily distributed	2
	Distributed	3
	Highly distributed	4
	Very highly distributed	5
Location dependent	No - no safeguards	0
	No - some safeguards	1
	No - safeguards	2
	No - heavy safeguards	3
	Yes - not protected	4
	Yes – protected	5

However, the rating of a certain aspect happens based on expert judgement and is difficult to quantify objectively.

Severity

Severity is the property to rate the impact of an attack. Aligned with work done in [23, 24], we introduce the following aspects to quantify severity. The rating itself is done by giving each aspect a score and taking the maximum value according to Table 4 as a rating number for the respective threat.

Table 4. Properties for Severity Rating

Severity class	Description	Properties					
		Availability of flight routine	*Air Traffic Control*	*Cost*	*Fatalities*	*"Flying Public"*	*Exposure of proprietary information*
1 – None	There is no perceivable impact on safety, flight regularity, or business interests.	No impact	Slight increase in ATC workload	0$	0	No effect on flight crew, Has no safety effect, Inconvenience	No impact
2 – Minor	There is a limited adverse effect on safety, flight regularity, or business interests.	Recoverable loss of redundancy or backup capability	Slight reduction in ATC capability or significant increase in ATC workload	0 - 10.000$	0	Slight increase in workload, Slight reduction in safety margin or functional capabilities, Minor illness or damage, Some physical discomfort	Disclosure of non-sensitive airline operation information
3 – Major	There is a serious adverse effect on safety, flight regularity, or business interests.	Significant flight delays	Reduction in separation or significant reduction in ATC capability	10.000 - 1.000.000$	0	Significant increase in flight crew workload, Significant reduction in safety margin or functional capability, Major illness, injury, or damage, Physical distress	Disclosure of some sensitive airline operation information
4 – Hazardous	There is a severe adverse effect on safety, flight regularity, or business interests.	Flight interruption	Reduction in separation or a total loss of ATC capability (ATC Zero)	1.000.000 - 10.000.000$	1-5	Large reduction in safety margin or Functional capability, Serious or fatal injury to small number, Physical distress or excessive workload	Disclosure of lots of sensitive airline operation information, some security information
5 – Catastrophic	There is a catastrophic effect on safety, flight regularity, or business interests.	Fleet reroute	Collision with other aircraft, obstacles, or terrain	>10.000.000$	> 5	Hull loss, Multiple fatalities	Disclosure of highly sensitive airline operation information, security information

Table 5. Applying the Rating System Onto Selected Threats

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					

Result

Now we can form the likelihood/severity matrix and introduce three levels of acceptance, again aligned with official norms [16].

Negligible – Green: The threat is known and accepted, but deemed harmless.

Medium – Yellow: No immediate actions must be done to hinder the occurrence of the threat, but the threat itself and its development will be looked at closely.

Dangerous – Red: The impact of a successful attack is not acceptable and thus direct counter measures must be introduced.

The entire rating process of all threats includes rating of all attributes of severity and likelihood and is thus a long process. In Table 5 we present the final outcome, whereas Table 6 and 7 include an overview of all ratings regarding severity and likelihood of all threats.

Table 6. Threat Severity Rating

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

Table 7. Threat Likelihood Rating

Factor	Threats							
	T1	T2	T3	T4	T5	T6	T7	T8
Elapsed Time	1	3	4	2	4	3	3	3
Expertise	2	3	3	2	4	4	4	3
Knowledge of System	2	3	3	2	3	4	3	3
Window of Opportunity	1	3	3	1	3	2	2	2
Equipment	1	2	2	1	3	4	2	2
Distributed Attack	2	4	3	2	3	3	2	1
Location dependent	1	2	3	2	3	4	3	3
Average	**1.4**	**2.9**	**3.0**	**1.7**	**3.3**	**3.4**	**2.7**	**2.4**
Rating	**2**	**3**	**3**	**2**	**4**	**4**	**3**	**3**

Discussion

As the scope of this paper is limited to the radio link in the LDACS subsystem, 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. For these classes we derived the following five objectives also identified in [8]:

- The operation of the LDACS system security functions shall not diminish the ability of the LDACS system to operate safely and effectively.
- The LDACS system shall support reliability and robustness to mitigate denial of service attacks.
- The LDACS system shall support message authentication and integrity to prevent message alteration attacks.
- The LDACS system should support encryption to mitigate eavesdropping.
- The LDACS system shall support entity authentication to mitigate impersonation attacks.

From the objectives we can now derive some ideas on security functions, aligned to the common criteria process, that are to be included in our LDACS IT security architecture.

Identification: We have to provide all participating entities of our system with a method ensuring that the subject is the entity it claims to be.

Authentication: Authenticity of communication partners as well as for user identification and authentication defines ways to prove the subjects identity.

Authorization: We have to provide methods in our IT security architecture to control the permissions granted to entities.

Encryption: Encryption will be mainly deployed for inter-entity user data confidentiality transfer protection, making use of cryptographic operations either using an asymmetric or symmetric encryption approach.

System Integrity: Integrity here refers to the correct and intended functioning of systems. We need to implement mechanisms to ensure that.

Data Integrity: This is related to mechanism for data authentication, inter-entity user data integrity protection during transmission, and replay detection by making use of cryptographic primitives.

Safety: Safety measurements include self-tests, functions for information flow control e.g. according to previously specified information flow control policies and approaches for general availability protection.

Robustness: Starting in the physical layer, protection against physical tampering and interference is key in achieving a reliable and robust system.

Secure Logging: Recording the occurrence of security relevant events, storing log data securely with non-repudiation and immutable properties and auditing via security review with data and tools only available to authorized users, helps to provide assurances that the defined policies and mechanisms work as intended.

Key Management: Secure cryptographic key management meaning key generation, key distribution, key access and key destruction as well as making use of the keys in cryptographic operations like encryption, decryption, generation or check of a cryptographic checksum for integrity, key agreement and so forth is an essential requirement for the success of most security functions.

How these functions are implemented is subject to future research.

Conclusion

As a promising candidate for the future communication infrastructure, LDACS was developed since 2007 and is currently in the process of being standardized.

In this paper we present a LDACS threat-and-risk analysis by introducing a suitable rating mechanism. By this we establish principles for a complete IT security architecture for LDACS. In the threat-and-risk analysis we found eight major threats and rated them according to our rating system. Seven out of these eight were classified as *hazardous*, one even with a *probable* likelihood. Based on that knowledge, we derived five objectives as protection goals for our assets and pointed towards corresponding security functions, which can help to achieve these goals.

The results are a promising basis to pave the way for a successful IT security architecture includable in the standardization process of LDACS. The next steps on the road ahead are to further define the security functions and to look for suitable places in the LDACS protocol stack to implement, test and evaluate them. 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 years to come.

References

[1] EUROCONTROL, “Challenges of Growth 2013 - Task 4: European Air Traffic in 2035,” 2013. [Online]. Available: http://www.eurocontrol.int/articles/challenges-growth.

[2] Michael Schnell, Ulrich Epple, Dmitriy Shutin, and Nicolas Schneckenburger. LDACS: Future Aeronautical Communications for Air-Traffic Management. IEEE Communications Magazine, 52(5):104–110, 2014.

[3] Mohamed Slim Ben Mahmoud, Alain Pirovano, and Nicolas Larrieu. Aeronautical Communication Transition from Analog to Digital Data: a Network Security Survey. Computer Science Review, 11:1–29, 2014.

[4] M. Sajatovic, B. Haindl, U. Epple, T. Gräupl, C. Rihacek, M. Schnell, N. Fistas, J.-U. Koch, H.-W. Kim, and E. Le-Ho, "Updated LDACS1 System Specification," SESAR JU, Brussels, Belgium, report EWA04-1-T2-D1, 2011.

[5] T. Gräupl, M. Ehammer, and C.-H. Rokitansky, "L-DACS 1 Data Link Layer Design and Performance," in Proc. Integrated Communications Navigation and Surveillance Conf., Arlington, VA, 2009.

[6] T. Gräupl, and M. Ehammer, "L-DACS1 Data Link Layer Evolution of ATN/IPS," in Proc. 30th Digital Avionics Systems Conf., Seattle, WA, 2011.

[7] O. Osechas, M. Mostafa, T. Graupl and M. Meurer, "Addressing Vulnerabilities of the CNS Infrastructure to Targeted Radio Interference," in IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 11, pp. 34-42, November 2017. doi: 10.1109/MAES.2017.170020

[8] Bilzhause, B. Belgacem, M. Mostafa, T. Gräupl, "Datalink Security in the L-Band Digital Aeronautical Communications System (LDACS) for Air Traffic Management," IEEE Aerospace and Electronic Systems Magazine, 2017.

[9] Eleventh Air Navigation Conference, "Report of Committee B on Agenda Item 7," Montreal, 2003.

[10] EUROCONTROL/FAA, "Action Plan 17 Future Communications Study - Final Conclusions and Recommendations," 2007.

[11] S. Brandes, M. Schnell, C.H. Rokitansky, M. Ehammer, T. Gräupl, H. Steendam, M. Gue-nach, C. Rihacek, and B. Haindl, "B-VHF - Selected Simulation Results and Final Assessment," in Proc. 25th Digital Avionics Systems Conf., Portland, OR, 2006.

[12] C. H. Rokitansky, M. Eham-mer, T. Gräupl, M. Schnell, S. Brandes, S. Gligorevic, C. Ri-hacek, and M. Sajatovic, "B-AMC A system for future Broadband Aeronautical Multi-Carrier communications in the L-Band," in Proc. 26th Digital Avionics Systems Conf., Dallas, TX, 2007, pp. 4.D.2-1 - 4.D.2-13.

[13] C.H. Rokitansky, M. Eham-mer, T. Gräupl, S. Brandes, S. Gligorevic, M. Schnell, C. Rihacek, and M. Sajatovic, "B-AMC – Aeronautical Broadband Communication in the L- band," in Proc. 1st CEAS European Air and Space Conference, Berlin, Germany, 2007, pp. 487-496.

[14] M. Schnell, S. Brandes, S. Gligorevic, C.-H. Rokitansky, M. Ehammer, T. Gräupl, C. Ri-hacek, and M. Sajatovic, "B-AMC – Broadband Aeronautical Multi-carrier Communica-tions," in Proc. Integrated Communications Navigation and Surveillance Conf., Bethesta, MD, 2008.

[15] Haindl, B.; Rihacek, CHr.; Sajatovic, M.; Phillips, B.; Budinger, J.; Schnell, M.; Lamiano, D. & Wilson, W. (2009). Improvement of L-DACS1 Design by Combining B-AMC with P34 and WiMAX Technologies, Integrated Communications Navigation and Surveillance Conference (ICNS 2009), Arlington, VA, USA, May 2009

[16] TCCR Agreement. Common criteria for information technology security evaluation part 1-3: Revision 4. NIST, page 93, 2012.

[17] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for Information Security Management. 2013.

[18] Tom Phinney. IEC 62443: Industrial Network and System Security. Last accessed July, 29, 2013.

[19] Mohamed Slim Ben Mahmoud, Nicolas Larrieu, and Alain Pirovano. Risk Propagation Assessment for Network Security: Application to Airport Communication Network Design. John Wiley & Sons, 2013

[20] Nicolas Giraudon, Marc lannes, Stéphane Tamalet, Marc Lehmann, Slim Ben Mahmoud, Nicolas Larrieu, Antonio Correas, and Stéphane Fasetta. Part 1 -AeroMACS Safety and Security Analysis, Part 2 - AeroMACS Security Analysis. Technical report, AENA, AIRBUS, DSNA, EUROCONTROL, INDRA, NATMIG, SELEX, THALES, 2014.

[21] Galileo Tamasi and Micaela Demichela. Risk Assessment Techniques for Civil Aviation Security. Reliability Engineering & System Safety, 96(8):892–899, 2011.

[22] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In International Conference on Applied Cryptography and Network Security, pages 253–271. Springer, 2013.

[23] Future Communications Study Operational Concepts and Requirements Team. Communications Operating Concept and Requirements for the Future Radio System. Standard, EUROCONTROL/FAA, 2007.

[24] Natalie Zelkin and Stephen Henriksen. L-Band Digital Aeronautical Communications System Engineering-Initial Safety and Security Risk Assessment and Mitigation. 2011.

[25] Stephen Henriksen and Natalie Zelkin. L-Band System Engineering-Concepts of Use, Systems Performance Requirements, and Architecture. 2011.

[26] ICAO Secretary General - 1999. Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN). Dot 9705an/956, International Civil Aviation Organization, 1999

[27] SRMGSA FINAL. Safety Risk Management Guidance for System Acquisitions. 2007.

[28] John Hird, Rainer Koelle, and Denis Kolev. Towards Mathematical Modelling in Security Risk Management in System Engineering. In Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013, pages 1–13. IEEE, 2013.

[29] Tobias Kiesling, Matias Krempel, Josef Niederl, and Jürgen Ziegler. A Model-Based Approach for Aviation Cyber Security Risk Assessment. In Availability, Reliability and Security (ARES), 2016 11th International Conference on, pages 517–525. IEEE, 2016.

Email Addresses

nils.maeurer@dlr.de

ab@sec.uni-passau.de

2018 Integrated Communications Navigation and Surveillance (ICNS) Conference

April 10-12, 2018