TOWARDS A MORE SECURE ATC VOICE COMMUNICATIONS SYSTEM

Tim H. Stelkens-Kobsch, Dr. Andreas Hasselberg, Dr. Thorsten Mühlhausen, Dr. Nils Carstengerdes, Michael Finke and Constantijn Neeteson, German Aerospace Center (DLR), Braunschweig, Germany

Abstract

Contradictory to communication safety in the aviation field communication security has received relatively little attention to date, although the threats regarding air traffic security have been rapidly increasing in recent years. Within the project GAMMA (Global ATM Security Management) the German Aerospace Center (DLR) is developing a prototype to support air traffic controllers (ATCO) in detecting intrusions into the air ground voice system and therefore allow subsequent mitigating actions to be conducted.

Introduction

Many significant accomplishments to secure Aviation have been reached in the last years. While much effort was spend to address the physical security, threats against its information infrastructure are not well covered [1]. For example the pilot-controller very high frequency (VHF) voice communication is open to masquerading intruders, which pretend to be air traffic controllers and give instructions to aircraft. While the problem has cached the interest of some researches [2] and was identified as threat in a study by Eurocontrol [3], it has not really attracted community's attention so far. On one hand this results from not causing crucial damages until now, on the other hand this is induced by the cautious policy of ANSPs (Air Navigation Service Providers). However, there is a significant number of attacks [1] and examples demonstrate, that they pose a real danger of confusing air traffic controllers and pilots [4] [5].

This paper describes the approach to develop a dedicated prototype for secure ATC communications, the risk assessment and the risk treatment regarding ATC communications as conducted in the ongoing GAMMA project using SESAR's methodology [6] and applying SESAR's Minimum Set of Security Controls (MSSC) [7].

In order to establish the context, the first part of the paper will describe the investigated system which is currently in use for air-ground radio communications in ATC. Further, the applied methodology to assess and treat the risks regarding the air-ground radio communication system will be explained. This will lead to the postulation of a prototype which will be built within the project GAMMA in order to increase resistance against the elaborated threats and to reduce the vulnerability of the system. Finally, the approach to evaluate the benefit of this prototype will be described and the paper will be completed with a discussion about the next steps and an outlook to the future.

Air Ground Communication in Air Traffic Control

In the present time, air-ground communication between ATC and aircrews is designated as 'aeronautical mobile service' as part of the 'international aeronautical telecommunication service'. Within the aeronautical mobile service, voice communications and data link communications can be distinguished [8]. For now data link communications are already implemented as CPDLC (Controller Pilot Data Link Communications) for exchanging messages in a non-time critical context. Further extension of using data link communications can be expected in the future. But due to several operational problems especially in a busy traffic environment, in non-standard situations or simply when exchanging air-ground messages in plain language, voice communication is still the basic and most important communication method within the aeronautical mobile service.

From the technical point of view, voice communication in aviation is done by using omnidirectional analogue radio transceivers. Civil ATC radio communication uses the VHF band within 117.975-137.000 MHz. Carrier waves are double-sideband and amplitude modulated. ATC ground stations work with a higher power output than

airborne stations and are designed to ensure sufficient radio coverage depending on operational demands [9]. ATC voice communication equipment has to be protected from unauthorized access in general [8].

Radio transmissions have specific wave propagation characteristics depending on the frequency, transmitter environment and transmitting method (directional, omnidirectional, etc.). VHF (Very High Frequency) transmissions require a radio line-of-sight to a certain extend; wave deflection effects play a minor role. This leads to the consequence that communication between two ground stations or between a ground station and a low flying aircraft might not be possible, depending on the distance and topography between them (Figure 1). Further, due to the omnidirectional transmission, the signal power decreases with distance, leading to a reduced communication quality with increasing distance due to background noise. Consequently, transmissions from distant stations can more easily be blocked out by other nearby stations.

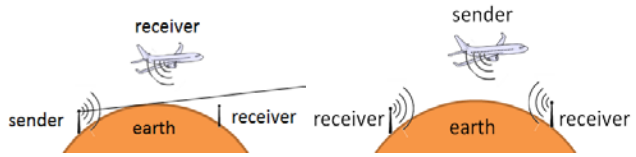

Figure 1: Line of Sight Dependency for VHF Transmissions. Left: Ground Receiver Does Not Track Sender. Right: Both Receivers Track Sender.

Depending on national regulations, VHF transmitters may only be operated with a specific approval by a national authority [10].

To take part in air-ground voice communications, a special knowledge regarding voice communication procedures and standard phrases as well as a sufficient language proficiency is required. Also depending on national regulations, a radio telephony certificate may be obligatory [11].

With regard to security, the air ground voice communication can easily be intruded due to general availability of aircraft radio transmitter equipment and its analogue, unsecured nature.

Risk Assessment

The overall process of risk identification and risk evaluation is called security risk assessment [12]. After assessing risks, it is possible to identify a set of security requirements which ensure that the consequences of an attack are known and managed and that the targeted asset can recover to normal operations in a reasonable time. The required main phases for the assessment of security risks are typically [12] (cf. Figure 2)

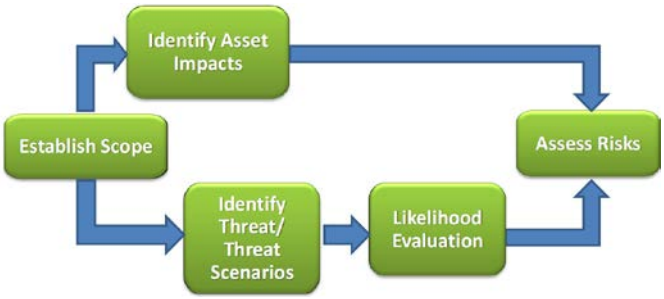

Figure 2: Typical Security Risk Assessment Process [13].

- to establish an accurate scope,
- to identify asset impacts,
- to identify threats / threat scenarios,
- to evaluate the likelihood of each threat / threat scenario,
- to assess the security risk.

When this process is completed it is followed by the definition of a set of security controls (treatment actions) and requirements to reduce the risk level of unacceptable risks to an acceptable level.

In the frame of SESAR a step-by-step guidance was developed which provides support for an operational focus area (OFA) to use the security risk assessment methodology (SecRAM). In Figure 3 the steps to execute the SecRAM methodology proposed by SESAR are represented graphically.

In the context of secure ATC communication the SecRAM methodology was applied to the air ground communication system currently used in air traffic control as described above.

This approach will be further described in the following sections (see also Figure 3).

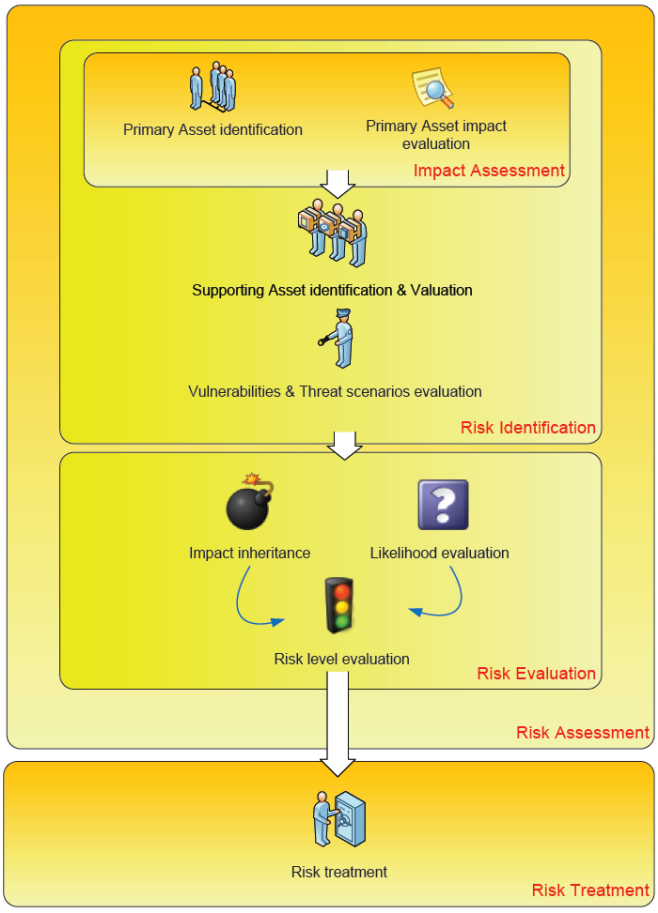

Figure 3: SecRAM Methodology [13].

Asset Identification and Valuation

The differentiation between primary assets and supporting assets has to be defined in advance of performing a risk assessment. Following [12], primary assets are for example intangible information and services which are of value to an OFA and which shall be protected. A successful attack would ultimately impair the primary assets and have an impact on the ATM system.

Supporting assets are entities which enable the primary assets. Supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets.

Primary Asset Identification

There are two types of primary assets which have to be protected: services and information (more precisely primary information).

Services may be further divided into services addressed by the OFA, system services, operational concepts and operational activities which are essential to keep the business mission running (solely or in combinations), contain secret processes or involve proprietary technology. Furthermore the necessary services to comply with contractual, legal or regulatory requirements have to be secured.

Information is considered as primary when it is (1) vital for the exercise of the mission or business, (2) personal regarding privacy issues, (3) strategic and/or confidential, (4) high-cost belonging to long time acquisition duration and/or high acquisition cost.

Impact Assessment

For each primary asset the required level of Confidentiality (C), Integrity (I) and Availability (A) has to be defined. Typically this is achieved by stating a number from 1 to 5 for each of the CIA criteria allocated to the asset. Thereafter, the impact regarding loss or degradation of the above stated criteria has to be evaluated in case of impact on the considered asset. Within GAMMA this was done using the SESAR security impact areas described in [12].

Supporting Asset Identification and Valuation

As stated earlier supporting assets are tangible elements that support the existence of primary assets. Entities involved in storing, processing and/or transmitting primary assets are classified as supporting assets. Examples are servers, databases, laptops and workstations [14]. When identifying supporting assets it has to be considered that each supporting asset is linked with one or more primary assets.

After applying the SESAR methodology, the supporting assets of the ATC communication system have been identified being the voice system, each individual aircraft, each en-route ACC (Air Traffic Control Center), each approach ACC and each airport tower.

Threat Scenarios

In order to act out possible threats affecting the assets of ATC radio communications, a list of threat scenarios relevant for the OFA has been elaborated. In order to establish the list it was assumed that a

threat scenario is the chain of events or occurrences which take place starting with a threat source and ending with the consequences of an incident. The scenario is originated by a threat source and exploits the vulnerabilities of a specific supporting asset for reaching the primary assets and compromising their level of confidentiality, integrity or availability [12].

Threat Sources Identification

Risk assessment proceeds with the next step which is intended to identify all possible threat sources which may exploit vulnerabilities of supporting assets in order to achieve their aim to compromise the system. Following the SESAR approach the process is performed by starting from two different origins: A vulnerability assessment of all supporting assets and a review of attackers and how they can attack a supporting asset. This step has a valuable impact on the development of security requirements as it is expedient to consider all possible threats to the ATM system. All threats which are not covered in this step will pose a high potential danger on the system, because they are unknown.

Though it is some kind of reading tea leaves the consideration of future threats is an immensely important task within this step of the risk assessment. One technique which shows to be effective in finding out new threats, threat agents and assets into the security viewpoint is horizon scanning [15]. For each time horizon the approach is to determine, detect and collect new threats/attack methods or assets. These time horizons may vary between a short term horizon over medium term horizon to long term horizon.

Threat Scenario Assessment

Within this part several threat scenarios shall be developed covering each selected, potential threat of the OFA. This includes the identification of the attacker and the attacked supporting asset as well as the detailing of the vulnerabilities of the supporting asset and the different means of the attack.

A major outcome of this assessment step is the development of concrete examples describing the threats, the vulnerabilities and the threat sources. The scenarios are described in narrative text and shall be coordinated with stakeholders.

Risk Evaluation

Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable. In this context the security risk is a combination of the impact of a successful attack and the likelihood that the impact will be achieved.

Impact Evaluation

The impact evaluation takes into account the situation with and without security controls in place to reduce the impact of an attack. This leads towards two different impacts attacks may have on the considered system: the inherited impact which describes the maximum impact a threat scenario would have without existing security controls and the reviewed impact which is to be expected when existing or planned security controls are taken into account for mitigating the impact of threats on the system. Consequently the reviewed impact is always equal or less then the inherited impact. When the reviewed impact is different from the inherited impact the causing security controls shall be listed and described.

Likelihood Evaluation

Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics). In this part of the assessment the likelihood that an attack is successful shall be estimated. When determining the likelihood the existing and planned security controls have to be taken into consideration. The scale to differentiate the probability of likelihood ranges from very unlikely to certain. This categorization helps to classify the severity of a potential attack resulting from a threat and the impact of a threat scenario on the system.

Risk Level Evaluation

The level of risk is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks. In the practical application within GAMMA this is applied to the generated threat scenarios in order to determine the risk level. For all threat scenarios, the risk level of a threat scenario follows an automatic calculation from

the reviewed impact and the likelihood of the threat scenario resulting e.g. from Table I. It has to be mentioned that there are different forms of risk level evaluation tables mentioned in literature but the 5x5 matrix shown in Table I was decided to be the most suitable because of its adoption by SESAR.

Table 1. Risk Level Evaluation [13]

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Security Objectives

Security objectives are derived from high level OFA policy objectives and are measurable statements of intent relating to the protection of a primary asset [12]. This means that the identified risks on primary assets are used as an input for a so called security objective report. Here the security objectives on primary assets are defined and compared with risk levels in order to decide if a distinct risk should be treated or is acceptable (also referred to as security needs).

Security objectives are again defined in terms of confidentiality, integrity and availability of the associated primary asset.

In order to determine the security objectives regarding the air-ground voice communication system the following approach has been chosen:

The possible impact of feared events on this system has been used to list the security objectives. Security needs, well known as the risk appetite, have then been calculated by confronting the level of risk of the identified threats with the security objectives.

The last step was performed as described in [14]. This step consists of the risk treatment by reducing the risk (with technical or procedural security controls), avoiding the risk (stop the function concerned by the risk), accepting the risk (with its consequences) or transferring it (the risk will be covered by another system/entity).

Risk Treatment

Risk treatment (as conducted in [14]) develops a set of security controls to ensure that the remaining residual risks after the risk treatment meets the aforementioned security objectives.

To achieve this, the risk treatment involves selecting and implementing one or more treatment options for identified risks and is therefore a process to modify or manipulate them. Once a treatment has been implemented, it becomes a control or it modifies existing controls. There are four options for risk treatment: risk reduction, risk avoidance, risk acceptance, or risk transfer [13]. The main concept of risk treatment is to select a list of prioritized risks from the risk evaluation step and define a risk treatment plan.

The Security Risk Treatment conducted in GAMMA can be summarized with the following steps:

- Collection of main inputs from the security risk assessment performed,
- Risk treatment prioritization,
- Association of the Minimum Set of Security Controls (MSSC) defined by SESAR to each risk identified,
- Refinement of SESAR MSSC and definition of additional security controls for every asset and threat scenario,
- Residual risk evaluation,
- Additional security recommendations.
- Security Key Performance Indicators (KPI)

One important component of the risk treatment is the application of the MSSC. The MSSC define a set of common-sense controls which all OFAs shall apply. These sets have been elaborated by SESAR [7] and applied during the risk assessment process in GAMMA. All resulting vulnerabilities were then investigated and additional security controls have been postulated which reduce the residual risks to tolerable levels. Thus the outcome of the risk treatment phase was a set of security controls which allow decreasing the vulnerability while increasing the security of the ATC air-ground communication in

the best way. The security controls have been further elaborated and resulted in the postulation of a prototype to be hooked up to the existing system.

The discussed prototype for securing ATC communications consists of three detector modules, namely speaker verification module, voice pattern anomaly detection module and conformance monitoring module, and one correlation module (see Figure 4). This prototype will be installed as well on ground in the controller working positions (CWP) of the air traffic controllers as in aircraft cockpits. The speaker verification module listens to the voice communication and identifies the speakers by comparing the voice signals to a stored acoustic fingerprint. The voice pattern anomaly detection module listens to the voice communication and identifies abnormal voice patterns (e.g. induced by stress). The conformance monitoring tool uses electronically available clearances and radar data as input and checks if the aircraft flight trajectories correspond to the instructions and the predicted regular behaviour.

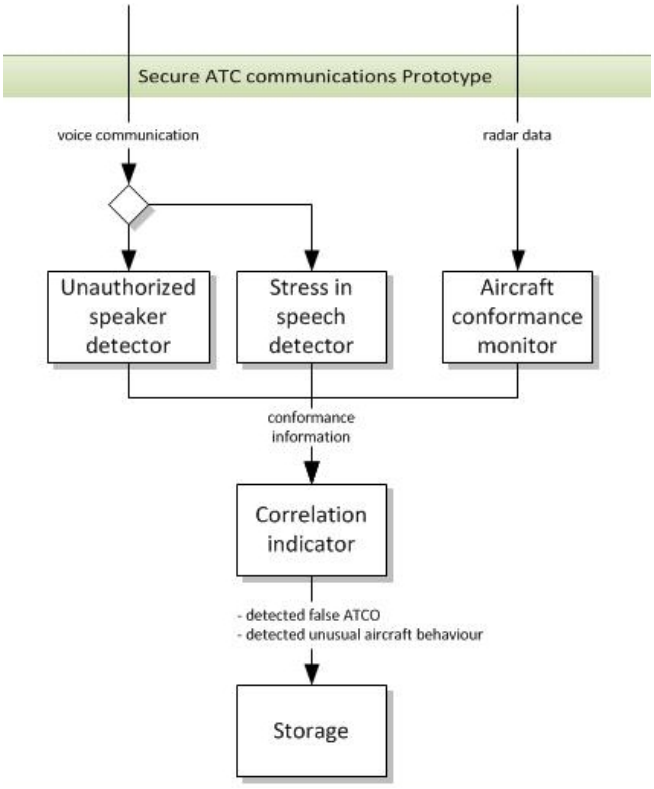

Figure 4: Logical View of a Prototype to Secure ATC Communications.

Additionally, the on-board version of the discussed secure ATC communications prototype is installed in cockpits. It consists of the speaker verification module and the voice pattern anomaly detection module and forwards its results to the likewise configured prototype located in the ATC Center. Based on the information from these sources the correlation module of the secure ATC communications prototype in the ATC Center decides if a false ATCO is detected. When such an intruder is identified, the result is made available to the ATCO and the cockpit crews in this sector.

At this point it has to be mentioned that a prerequisite for a successful implementation of the proposed prototype should be the transition of air-ground ATC communication from analogue to digital technique, which would immensely support the chances of a secure ATC radio communication system.

Approach to Benefit Evaluation

In chapter V, the prototype for secure ATC communications was introduced. This prototype will be validated according to phase V2 of the European Operational Concept Validation Methodology (E-OCVM, [17]) to gain initial feedback regarding its acceptance and its benefit. Whereas phase V0 and V1 of the E-OCVM Concept Lifecycle Model (CLM) define the air traffic management needs and the scope of the concept, phase V2 explicitly addresses feasibility and recommends validating the concept regarding operational user acceptance and operability.

Within the planned validation activities described in this paper, the herein discussed prototype will be validated as a single prototype without connections to other security systems also developed in the GAMMA project.

As the prototype is developed to support certified controllers in the detection of false ATCOs, the validation should provide evidence that the detection of false ATCOs is improved when support by the prototype is installed. Therefore, the first validation objective is to improve the detection of a false ATCO by utilising the prototype. Furthermore,

the situation awareness about attacks of false ATCOs should be improved. Thus, the second objective is to validate that the solution leads to a better situational awareness of as well controllers on ground as cockpit crews in the sector regarding occurrence of a false ATCO.

The acceptance of the secure ATC communications prototype by controllers is one of the crucial issues on hand. If it is not accepted, air traffic controllers will probably not use it or may ignore it. They will only accept such a kind of system, if it is useful and trustworthy in their opinion. Therefore, the third objective of the validation is to validate that the performance of the prototype is acceptable (regarding false alarms, correct detection, usefulness and trust)

To collect feedback for the prioritization of further development effort, the prototype should be validated not only as a whole but the individual modules should be assessed each separately. Thus, the fourth validation objective is to compare the impact of individual prototype subsystems on threat management (speaker verification (SV), voice pattern analysis (VPA) and conformance monitoring (CM)).

In order to conduct the validation exercise, some assumptions have to be made about the operational environment, in which the proposed prototype shall be applied.

- MSSCs are considered as already implemented.
- Secure ATC communication prototype is installed at controller and pilot side.
- False ATCO has enough knowledge and the necessary equipment to provide logical instructions to the aircraft.
- ATC clearances are electronically available and can be used as input for the prototype.
- Speaker verification module has access to acoustic fingerprint of pilots and controllers.
- Speech data during validations is of high digital quality (VoIP), the minimal sampling rate and minimal bits per sample will be defined at a later stage.
- Aircraft prototype for secure ATC air-ground communication is able to downlink indicators to ATC and receive uplinked indicators to the cockpit crews in the sector.

A human-in-the-loop real-time simulation consisting of reference and solution runs will be used as a method to validate the improvements regarding the detection of the false ATCO threat by using the proposed prototype compared to current operations.

During these simulation runs, the real air traffic controller will be faced with a multitude of events. These are (1) valid pilot behaviour, (2) pilot error which is not false ATCO induced, and (3) pilot behaviour induced by instructions from a false ATCO (e.g. false ATCO induced readback, unusual trajectory). Furthermore, the possibility of the real controller to hear the false ATCO will be varied. (4) Half of the instructions from the false ATCO will be audible for the real controller. (5) The other part of the instructions of the false ATCO will only be audible for the pilots, but not for the real controller (simulating the radio line-of-sight issues described in chapter II). The following event categories are therefore defined

Event A) Valid pilot behaviour

Event B) Pilot readback error (not induced by false ATCO)

Event C) Pilot behaviour error (not induced by false ATCO)

Event D) False ATCO induced behaviour (instructions from false ATCO audible for real ATCO)

Event E) False ATCO induced behaviour (instructions from false ATCO not audible for real ATCO)

For each event, the real controller participating in the validation exercise has to decide if this event is induced by a false ATCO or not. Therefore, a detection rate, a detection time and a false alarm rate is calculable.

One additional task of the real controller is to detect unusual trajectories. If such a trajectory is detected, the real controller has to give corrective commands. For this kind of detection, a detection

rate, a detection time and a false alarm rate are calculable. Furthermore, the acceptance of the security assistance prototype will be evaluated (including the false alarm and correct detection rate of the prototype, the usefulness of the prototype and the trust in the prototype).

In the baseline, the ATCO will receive no decision support by any system in judging the events. In the solution runs the ATCO will get support by the proposed prototype. The solution will be validated in four separate runs, one run for each detection subsystem of the prototype (speaker verification module; voice pattern anomaly detection module; conformance monitoring module) and one run with the prototype as a complete assistance system (incl. correlation indicator) active. Thereby, the individual benefit of each prototype module can be assessed.

Next Steps and Outlook

The above described system is aimed at improving the security of ATC communication at a single ATC center. But within the GAMMA platform it is only one component as there also exist other security threats like GNSS spoofing and jamming or satellite communication disruption (referred to as local security systems in Figure 5). The complete system postulated by GAMMA is depicted in Figure 5 where LGSOC means “local GAMMA security operation center”, NGSMP means “national GAMMA security management platform” and EGCC means “European GAMMA control center”. In a next step, some of the components will be combined to support the risk mitigation for coordinated attacks to the ATM system. In a final step all GAMMA components will be combined and connected by a security management platform, which will collect all available information from the different components and provide national and/or international authorities with assistance in decision making about countermeasures.

In aviation, reaction time to an incident is crucial and normally very short. Concerning safety critical incidents, two main components can be differentiated:

- The detection of a potential dangerous situation
- The elimination of this situation with countermeasures (mitigation)

Although GAMMA provides also mitigation measures, the main focus lies on detection. A fast and reliable detection of the threats is essential. Therefore, the modules of ATC communication component will run through a continuous improvement process based on the above described validation procedures. Especially the conformance module has a high potential to improve the awareness of unsecure situations. Nevertheless, further research in situational and location dependent typical aircraft behavior and its implementation is required to make conformance monitoring assessment and controller assistance reliable. Considering the second component (mitigation), secure ATC air-ground communication and other security prototypes result in faster detections of security threats. This, in turn, offers more opportunities to mitigate those situations due to more options for actions and/or earlier start of countermeasures. Besides, information gathered by one security prototype can be transmitted to other prototypes and ATM actors in order to increase the awareness concerning possible distributed attacks. Ultimately this may prevent attacks. Eventually the reaction to the detected threat is often depending on national legislation and sovereign power. Fast reaction (especially cross border) needs additional international cooperation, which is far beyond the focus of the GAMMA project. Although measures might be confidential, further international research in this area is strongly encouraged to reduce the security threats of the future.

References

[1] Iasiello, Emilio. "Getting Ahead of the Threat: Aviation and Cyber Security." AEROSPACE AMERICA 51.7 (2013): 22-25.

[2] Prinz, J., M. Sajatovic, and B. Haindl. "S/sup 2/EV-Safety and Security Enhanced ATC Voice System." Aerospace Conference, 2005 IEEE. IEEE, 2005.

[3] Eurocontrol, VHF Security Study, Final Report, available: www.icao.int/safety/acp/Inactive%20working%20groups%20library/ACP-WG-N-SWG4-1/sgn04-01-misc01.doc

[4] LiveATC. (2011). 25-MAY-2011 Fake ATC in Action (LTBA-ISTANBUL). Available: http://www.liveatc.net/forums/atcaviation-audio-clips/25-may-2011-fake-atc-in-action-%28ltba-istanbul%29

[5] Chivers, H., J. Hird. (2013, September). "Security Blind Spots in the ATM Safety Culture". Presented at 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany

[6] EUROCONTROL ATM Security Risk Management Toolkit, ATM Security Risk Assessment Methodology, EUROCONTROL, Edition 1.0, May 2008.

[7] Minimum Set of Security Controls, SESAR Project 16.02.05, D05-006, Edition 00.06.00, August 2013.

[8] Communication Procedures including those with PANS status, ICAO Annex 10, Vol. 2, 6th Edition, July 2001.

[9] Communication Systems, ICAO Annex 10, Vol. III, 2nd Edition, July 2007.

[10] German Telecommunications Act, Effective from 22nd July 2004, revised 25th July 2014.

[11] German Regulation on Aeronautical Radio Telephony Certificates, Effective from 20th August 2008, Revised 7th August 2013.

[12] SESAR ATM Security Risk Assessment Methodology, SESAR Project 16.02.03, D02, Edition 00.01.01, January 2012.

[13] SESAR ATM SecRAM Implementation Guidance Material, SESAR Project 16.02.03, D02, Edition 00.02.06, February 2013.

[14] D2.3 - Risk Treatment Report, GAMMA Project, D2.3, Final Version, January 2015.

[15] D2.1 – Threat Analysis and Evaluation Report, GAMMA Project, D2.1, Final Version, January 2015.

[16] D4.1 – ATM Security Requirements, GAMMA Project, D4.1, Final Version, March 2015.

[17] E-OCVM, European Operational Concept Validation Methodology E-OCVM, 3rd Edition, February 2010

Acknowledgements

The research leading to the results presented in this paper has received funding from the European Union FP7 under grant agreement n° 312382.

More information can be found in www.gamma-project.eu.

Email Addresses

Tim H. Stelkens-Kobsch: tim.stelkens-kobsch@dlr.de

Dr. Andreas Hasselberg: Andreas.hasselberg@dlr.de

Dr. Thorsten Mühlhausen: thorsten.muehlhausen@dlr.de

Dr. Nils Carstengerdes: nils.carstengerdes@dlr.de

Michael Finke: michael.finke@dlr.de

Constantijn Neeteson: Constantijn.neeteson@dlr.de