SECURITY IN ATM – A VALIDATION APPROACH FOR SECURITY PROTOTYPES

T. H. Stelkens-Kobsch, M. Finke
Deutsches Zentrum für Luft- und Raumfahrt (DLR), Lilienthalplatz 7, 38108 Braunschweig, Germany

Abstract

The insights presented in this paper are outcomes of an ATM security research project that was invented to collect and bundle the latest knowledge gathered in the Air Traffic Management Security domain. As well the concept as the validation of a holistic security management approach (considered as a whole and divided into separate sub-systems) is evaluated and developed. Due to the big perimeter of the project the study presents an excerpt from the work done. Therefore the paper describes a possible security prototype validation methodology which was developed within the project, which is furthermore underpinned with its adaption to a security prototype intended to enhance security of the air traffic control voice communication system.

1. INTRODUCTION

Thanks to the Single European Sky ATM Research Programme (SESAR) and the Next Generation Air Transportation System (NextGen), the Air Traffic Management (ATM) community has access to a bunch of tools and methodologies to tackle various problem areas belonging to the ATM of the future. Although SESAR has also created the basis for validation regarding functionality of security prototypes, extensive validation expenditures in respect to tools, systems or prototypes in the ATM security domain have not yet been realized. This is indeed an emerging task when introducing security tools to ATM.

The emerging challenges in the next generation ATM when looking at security still seem to be underestimated. This stems from the fact that ATM, when being addressed as a system of systems, not only gives attention to threat sources like those well-known from the cyber security area, but also to ATM specific sources like e.g. satellite communication or Air Traffic Control (ATC) radio communication. In order to establish security management tools in the ATM domain the Global ATM Security Management Project (GAMMA[1]) started in 2013. The main goal of the project is to develop ideas to solve emerging air traffic management vulnerabilities. This intention is backed up by practical proposals for implementation.

The paper will discuss a subset of the GAMMA project outcomes. This will especially deal with the Secure ATC Communications Prototype (SACom). The prototype will be used as an example to enrich the theoretical presented background with a more tangible contribution.

Although the project is still on its way there have already been some first insights into the validation phase as several rehearsals already took place. These insights will be described in more detail in the paper. Furthermore the theoretically delivered security prototype validation approach will be mapped to the prototype at hand. The obtained results will be presented and a discussion of the first validation results will be executed.

This paper therefore describes as well the postulated security prototype validation methodology as the application of the described methodology on a dedicated prototype for secure ATC voice communication. This may be used as the blueprint for validating other ATM security oriented systems.

2. THE GAMMA PROJECT

The project GAMMA [1] aims at building a global solution for ATM Security. Following a context establishment of the project´s goals a thorough analysis of the ATM system vulnerabilities has been undertaken right after the start of the project. Thereafter the possible threats trying to exploit the vulnerabilities were collected and their likelihood evaluated and balanced. In order to achieve this, the Security Risk Assessment Methodology (SecRAM), prepared and provided by SESAR, was applied the first time. The continuative work in the project focuses as well on the methodological approach for validating ATM security prototypes as on the development of designated security prototypes themselves.

Throughout the air traffic management system a mismatch between available techniques, utilised systems and approach to highest security standards is present. In recent years different new ATC means have been introduced (ADS-B, MLAT, A-SMGCS, CPDLC, etc.) or will be invented in the near future. Thanks to the efforts of previous years and the introduction of Safety Management to ATC [2], these systems are already fully developed from the safety perspective. On the other hand there often exists a clear lack regarding security issues. There are several sources of literature discussing the vulnerabilities of existing components of the ATM system [3]; a management system comparable to safety management is not yet fully developed and implemented.

[1] GAMMA, http://www.gamma-project.eu. The research leading to the results presented in this paper has received funding from the European Union’s Seventh Framework Programme under Grant Agreement n° 312382.

This paper will discuss the ATC radio communication system and introduce the security prototype SACom which shall help to secure the voice communication in the ATM. Later on it will be described how the first attempts to establish a validation methodology to validate ATM security prototypes have been undertaken in GAMMA. Finally the first validation results of the prototype SACom will be discussed.

3. ANALYSIS OF THE ATC RADIO COMMUNICATION SYSTEM

The ATC radio communication system was originally invented to allow safe control and maneuvering of aircraft throughout the responsibility area of air traffic control. It is true, that Controller Pilot Data Link Communication (CPDLC) and other data link based communication means are used more often nowadays. However, data link based communication means are mainly used for transmitting clearances and information which are not time critical (IFR clearances, area control of IFR flights enroute). Looking at the current situation air traffic control will continue to depend heavily on voice communication also in the (near and far) future.

The operation of very high frequency (VHF) transmitters is depending on national regulations and may need a specific approval by a national authority [4]. Prerequisites for taking part in air-ground voice communications are special knowledge regarding voice communication procedures and standard phrases as well as sufficient language proficiency. Also depending on national regulations, a radio telephony certificate may be obligatory [5].

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. To ensure proper functioning of VHF communication a high quality signal must be ensured. A partial or full Denial of Service (DoS) is for example simply achieved by simultaneous use of frequency. Simple authentication procedures are not applied for civil ATC voice communication applications as they are time and capacity consuming. When the VHF communication is interrupted intentionally or unintentionally the loss of communication may lead to severe damages especially in airspaces with high traffic load.

4. THE SECURE ATC COMMUNICATION PROTOTYPE

The invention of a secure ATC communication prototype is based on the evaluation of a number of relevant indicators which help to identify abnormal processes, procedures, operations and patterns in ATC [6]. With the provided prototype the controllers and pilots receive a bundle of tools to get information about these collected indicators and their evaluation. This shall help the involved people to isolate the attack and, if the system robustness is not sufficient, to furthermore reduce the effects of the attack in a resilient manner.

The SACom prototype consists of four main modules. The modules are listed below together with the ATM participant they are intended to support:

- Speaker verification → assistance for the pilot.
- Stress detection → assistance for the controller (and possibly the pilot).
- Conformance monitoring → assistance for the controller.
- Conflict detection → assistance for the controller.

Speaker verification and Stress detection use voice analysis algorithms and deliver a score value between 0 and 100.

Conformance monitoring and conflict detection are already well-developed systems and are typically used to increase safety in ATM. Nevertheless these indicators never have been applied in the ATM security domain and deliver valuable supporting information when applied in a security application. The effectivity of both supporting systems is furthermore greatly enhanced when used together with a speech recognition system. This has been proven with the very first experiments testing the prototype. These components of the SACom prototype are additionally used in combination with a speech recognition system which has been invented in a different project called AcListant [7].

5. DEVELOPMENT OF A SECURITY PROTOTYPE VALIDATION METHODOLOGY

When thinking about set up and construction of security prototypes it is mandatory to validate their functionalities in advance (“are we building the right system”, [8]). It is therefore needed to make the expected benefit tangible and not only to verify if the system was built right. The question is: are the newly introduced systems and functions (respectively processes) worth implementing?

The guidance material elaborated by SESAR and NextGen is well appreciated and worth implementing. Nevertheless up to now there is little to none availability of validation knowledge regarding validation of security prototypes and/or concepts.

One of the main aims of GAMMA is to translate the available SESAR guidance into applicable validation procedures. These procedures can then be applied to validate tools and systems, which have been built to increase security in the boundaries of the ATM system. To achieve this, the work in GAMMA follows a top down approach when applying the security risk assessment provided by SESAR [9].

After the most feared threats (threats resulting in highest damage) have been identified, the SecRAM methodology was applied which resulted in a structured investigation beginning with the definition of security objectives. The definition phase was followed by an analysis of existing risks (impact and probability of threat scenarios, deduction of security risk level) and a treatment of the risks. Hereafter the definition of security controls followed.

The security controls were identified by combining the SESAR Minimum Set of Security Controls (SESAR MSSC, [10]) with a definition of additional technical, organisational or procedural security controls.

The final step was the definition of ATM security key performance indicators (KPI). These KPI can be used to evaluate the efficiency of identified security controls. The KPI defined in GAMMA do not claim to be the complete set of indicators but are a good starting point to establish a standard to rate security controls, tools and systems for ATM security.

Summing up the above a successful approach to develop and validate ATM security prototypes consists of the following steps:

- Identify the primary and supporting assets
- Identify vulnerabilities
- Invent the attack scenarios
- Name the security objectives
- Analyse and treat the risks
- Define security controls
- Define Security KPI to quantify the efficiency of the security controls.
- Set up the validation plan
- Conduct the validation exercises

In the next chapters the application of this methodology is described using the SACom prototype as an example.

6. METHODOLOGY APPLICATION - FIRST VALIDATION RESULTS

6.1. Validation Exercise Description

According to the described security prototype validation methodology, the security KPIs listed in Table 1 were specified to validate the developed functionality of the SACom prototype and its modules.

As the prototype is designed to support air traffic controllers in handling a security incident, a real-time human-in-the-loop simulation was identified to be the best implementation for the validation. Due to several reasons an ATC simulation of the Düsseldorf Approach Sector was chosen. Active air traffic controllers from the DFS were (and will be in the near future) invited to take part in the exercises and were tasked to guide arriving IFR traffic to the ILS final runway 23R. No departing traffic and no VFR traffic was considered, as the pilot-ATC interaction is the focus of validation, while the distinct ATC procedure (belonging to VFR or IFR) is out of scope. For the same reason it is not foreseen to repeat the validation also for aerodrome control (tower control, ground control) in the current phase of the development.

Table 1: Security KPI identified/defined for SACom

Security KPI	***SACom functionality***
False Alarm rate	Speaker Verification
Detection rate	Speaker Verification
False Alarm rate	Stress Detection
Detection rate	Stress Detection
False Alarm rate	Conformance Monitoring
Detection rate SACom	Conformance Monitoring
Detection rate ATCo[2]	Conformance Monitoring
False Alarm rate	Conflict Detection
Detection rate SACom	Conflict Detection
Detection rate ATCo	Conflict Detection
Time until detection of unusual aircraft behavior	Conformance monitoring
Acceptance (Usability and Trust)	SACom as a whole

The validation exercises consist of several sessions, whereas each session of the validation exercise contains the following steps:

1) Briefing of the test person:

   The test person receives a theoretical introduction to the steps of the validation session, the ATC equipment to be used and basic information about the background of the exercise.

2) Speaker verification enrollment

   The test person gives an example of his or her voice by reading a prepared text, which is then recorded and converted into a valid enrollment. Afterwards, the quality of the created enrollment itself is checked by comparing speaker verification score values of all speakers, again with predefined utterances.

3) Simulator Training

   In this step, the test person has the opportunity to get familiar with the used simulator. The person shall furthermore practice to use the airspace and local procedures in the frame of a 15-30 min simulation with low traffic load. This simulation is done without any use of the SACom prototype.

[2] ATCo: Air Traffic Controller

4) Short Simulations

During a total number of 20 short-time simulations (3-5 min per scenario), the test person is confronted with a predefined traffic situation which also contains a predefined safety / security event. This event may lead to a critical deviation of any aircraft from the given clearance. The simulation is done without any support from the SACom prototype, but the prototype is nevertheless already active in the background to enable a direct comparison of the performance of the controller and the detection system in post processing.

5) SACom Briefing

The test person is theoretically introduced into the SACom system, its purpose and the concept behind its development. Other items which the test person shall get used to are the functionalities of the prototype and the corresponding indications.

6) SACom Training

In this step, the test person shall familiarise with the SACom indications (aircraft deviations, conflicts, speaker verification). During this training, the test person handles air traffic in the frame of a 15-30 min simulation. Several events (lateral deviation from flight path, vertical deviation from flight path, uninstructed turns, etc.) will be simulated by a random choice; these events trigger one of the corresponding detection functions of the SACom prototype.

7) Long simulation

This simulation lasts about 40 min and the test person will at first handle normal air traffic. After 10 min of runtime, an unauthorized person will intrude the pilot-ATC voice communication. The intruder will issue unauthorized ATC instructions in a defined time interval. The ATCo shall not hear the intruder as this simulates terrain shading effects. After 20 min of attack, the unauthorized person will cease to interfere. For 10 more minutes, the air traffic will continue as usual.

8) De-Briefing and Questionnaires

The test person gets the opportunity to give qualitative feedback about the exercise itself, the SACom prototype and impressions. Additionally, the test person will be asked to answer standard questionnaires dealing with situational awareness, trust and usefulness.

The design of the exercise allows both, quantitative and qualitative conclusions about the SACom prototype and can be used to collect representative data for all listed KPIs.

The main challenge when developing the simulation is to establish comparability for all sessions with all invited test persons. Air traffic simulations are often very dynamic due to the number of possibilities to handle the traffic and due to the individual ways of working. Experiences from previous simulations show that ATC simulations can develop very differently even if the boundary conditions as well as the traffic scenario are exactly the same. Therefore the main reason for designing a number of short simulation scenarios with predefined events was to reduce these effects to a minimum.

Other major challenges were to reduce adaption effects due to raised expectations of the test persons and to maintain the surprising effects. These items do have a close connection to establish repeatability of the simulations. This means: If the data gathered during simulations is not comparable due to changing boundary conditions the final evaluation is difficult if not impossible.

6.2. First Results and Discussion

The following chapters describe in detail the values which are evaluated during the validation exercises of the prototype SACom and how they are used to assess the mentioned KPIs.

6.2.1. Speaker Verification

The False Alarm Rate for the speaker verification can be defined as:

$$FAR_{SV} = \frac{\sum \text{Incorrect Speaker Alarms}}{\sum \text{All Speaker Alarms}} \quad (1)$$

where

- The term “Incorrect Speaker Alarms” refers to the sum of authorized utterances which did not reach the speaker verification score above an alert threshold.
- The term “All Speaker Alarms” refers to the sum of all analyzed transmissions with a score at or below an alert threshold.

The Detection Rate for the speaker verification can be defined as:

$$DR_{SV} = \frac{\sum \text{Detected unauthorized utterances}}{\sum \text{All unauthorized utterances}} \quad (2)$$

where

- The term “Detected unauthorized utterances” refers to the sum of unauthorized utterances whose verification score did not reach a speaker verification score above an alert threshold.
- The term “All unauthorized utterances” refers to the total number of utterances that were spoken by the unauthorized speaker.

These rates were determined within the exercise step 2) (Speaker verification enrollment). After an enrollment was successfully created, the test person and all other involved persons who take the role of an authorized speaker were asked to read a predefined number of prepared utterances while the speaker verification module collected score values for each utterance. Additionally, the unauthorized speaker also read a predefined number of utterances.

The results can be displayed as a graph where the x-axis shows the speaker verification scores and the y-axis shows the relative frequency of the distinct score value.

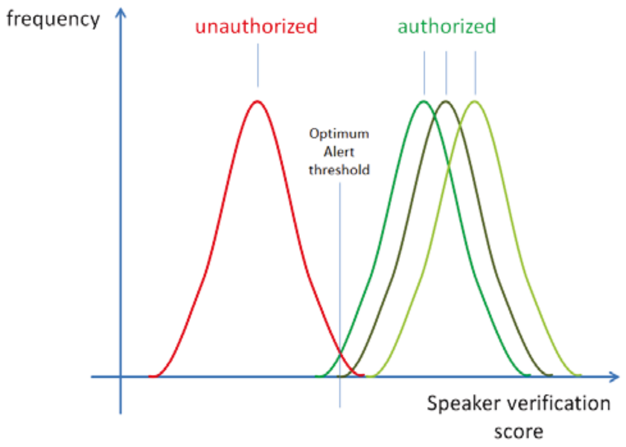

Figure 1: Expected result distribution - speaker verification

The anticipated result is that the evaluation of each speaker´s utterances shows a „Gaussian bell “around a distinct value. It is expected that all authorized speakers show a higher x-value, whereas the unauthorized speaker show a lower x-value for the speaker verification score (see Figure 1).

It is obvious that both, the FAR_{SV} as well as the DR_{SV} directly depend on the alert threshold which has been set. If this threshold is set to a lower score, the false alarm rate but also the detection rate will be lower. If the threshold is set to a higher score, then both, the false alarm rate and the detection rate will be higher. The conclusion is that the alert threshold needs to be set to the optimum score before starting the validation runs (Figure 1).

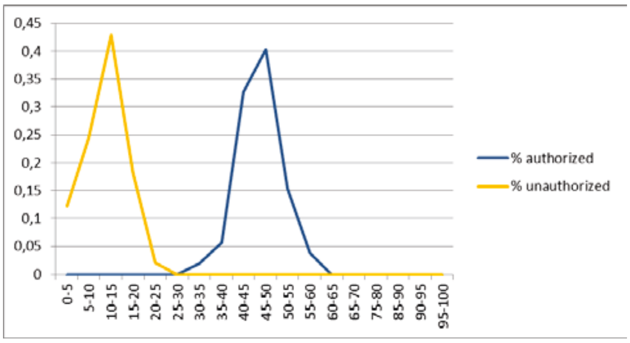

Figure 2: Speaker verification distribution (03.08.2016)

Figure 2 gives an example of this procedure with results from a validation trial that was conducted on August 3rd, 2016 at DLR premises in Braunschweig. During this validation trial the highest speaker verification score of the unauthorized speaker was 20 while the lowest speaker verification score of the authorized speakers was 33, which means that any alert threshold setting between 20 and 33 would have clearly separated the unauthorized speaker from the authorized speakers for all utterances that were spoken.

6.2.2. Stress Detection

For evaluating the stress detection module of SACom the False Alarm Rate is defined as:

$$FAR_{SD} = \frac{\sum \text{Incorrect Stress Alarms}}{\sum \text{All Stress Alarms}} \quad (3)$$

where

- The term “Incorrect Stress Alarms” consists of the sum of calm spoken utterances which were erroneously identified as stressed.
- The term “All Stress Alarms” refers to the sum of all analyzed transmissions with a score at or above the alert threshold.

The Detection Rate for stress is then defined as:

$$DR_{SD} = \frac{\sum \text{Correct Stress Alarms}}{\sum \text{Utterances Under Stress}} \quad (4)$$

where

- The term “Correct Stress Alarms” consists of the sum of correct identified utterances spoken with stressed voice.
- The term “Utterances Under Stress” refers to the total number of utterances that were spoken with stressed voice.

Analysing stress inherits the challenge that initially the provocation of stress is very difficult. The existence of real stress depends on several factors which are not easy to be unleashed artificially. Nevertheless, in order to be able to set up an evaluation procedure it has to be guaranteed that some radio communication utterances are definitely stressful. This leads to the following simplification:

- A stress alarm is defined as a stress score exceeding a distinct threshold.
- The long simulation run (exercise step 7) is used to evaluate the false alarm rates and the detection rates for the stress detection.
- A basic assumption states that before the simulated incident happens the situation is seen as calm and relaxed. This means that all available indicators are interpreted to replicate a situation without any stress and no utterances with stressed content exist for instance. The calm situation has to be kept for ten minutes.

- It is further assumed that during the incident respectively shortly after the beginning of the incident all participating speaker show an increased stress level (i.e. all utterances are stressed).

When looking at the very first validation results regarding stress detection, the (simulated) situation to cause stress and the level of the stress score could only be associated by chance. Possible reasons for this are the sophisticated training of air traffic controllers and their balanced nature itself, which may also be stated for professional pilots. Also aggressors seem to be resistant against stress (at least when the aggressors are acted by scientists or people without bad intentions).

At least the challenge to distinguish between stress caused by excitement (e.g. very first flight as a professional pilot in command), stress caused by high workload or stress caused by other "normal" reasons from stress resulting from precarious and unlawful intervention in air operations is not yet solved.

6.2.3. Conformance Monitoring

The False Alarm Rate for the conformance monitoring of SACom is defined as:

$$FAR_{CM} = \frac{\sum \text{Incorrect Deviation Alerts}}{\sum \text{All Deviation Alerts}} \quad (5)$$

where

- The term "Incorrect Deviation Alerts" is the sum of deviation alerts which were erroneously identified as deviations.
- The term "All Deviation Alerts" refers to the sum of all deviation alerts issued.

At this point the deviation itself has to be defined in order to use equation (5):

- A vertical deviation is detected when the discrepancy between expected value and present value is greater 300 ft.
- A lateral deviation is detected when the discrepancy between expected value and present value is greater than the standards defined by performance based navigation (PBN).
- A speed deviation is detected when the discrepancy between expected value and present value is greater than 40 kt (this value has been determined by the test management).

Equation (5) is just applicable for the SACom prototype and not for the work of the ATCo because it is assumed that the ATCo is always able to correctly judge if the aircraft behavior corresponds with the given clearances..

In contrast it is again possible to compare the DR of SACom and the ATCo. The Detection Rate for Conformance Monitoring may be defined as:

$$DR_{CM} = \frac{\sum \text{Correctly Detected Deviations}}{\sum \text{All Deviations}} \quad (6)$$

where

- The term "Correctly Detected Deviations" consists of the sum of correctly detected deviations.
- The term "All Deviations" refers to the sum of all occurred deviations.

In order to validate the conformance monitoring module the short scenarios as described in chapter 6.1 are used. During the different validation scenario runs just the pre-defined deviations as specified in the script for each distinct scenario are performed. If other deviations occur unintentionally, these have to be documented by the validation exercise observer. The observer also has to write down, when these unintentional deviations are detected by the ATCo. Consequently the term in the denominator of equation (6) is the sum of pre-defined deviations and deviations documented by the validation exercise observer.

The data collected by SACom is stored in a dedicated data base for later interpretation and comparison. It has to be considered that deviations might occur which are neither detected by the SACom nor by the ATCo. These deviations have to be identified by replaying and analyzing the relevant validation exercise run and it needs to be assessed manually if it was a false alert, a correct alert or another event such as an error of the speech recognition system or a wrong ATCo input.

First validation results show comparable DR values of both ATCo and SACom of about 90%. The FAR of the SACom is around 7%.

The time until detection, the "Detection Speed", of a non-conformant situation in air traffic is very critical. The shorter this time until detection, the more time is available to clear the situation. In order to determine the time until detection a replay of each occurred deviation has to be done to register the time of initial occurrence. The time of detection by the ATCo is noted by the validation observer and the detection time of SACom can be extracted from the connected database. The differences are then a measure for the "Detection Speed":

$$DS_{CM} = T_{\text{Detection}} - T_{\text{Initial Occurence}} \quad (7)$$

The smaller the obtained value for DS the more time is available to clear the situation. Equation (7) also allows distinguishing which deviations (vertical, lateral, speed …) are detected earlier by SACom then by the ATCo and vice versa. The evaluated average value for $DS_{CM,ATCo}$ is 40.6 seconds and for $DS_{CM,SACom}$ is18.9 seconds.

6.2.4. Conflict Detection

To evaluate the performance of the conflict detection module the “False Alarm Rate” can be defined as:

$$FAR_{CD} = \frac{\sum \text{Incorrect Conflict Alerts}}{\sum \text{All Conflict Alerts}} \quad (8)$$

For the sake of simplicity equation (8) may be re-written as:

$$(9) \quad FAR_{CD} = \frac{\sum \text{All Conflict Alerts} - \sum \text{Correct Alerts}}{\sum \text{All Conflict Alerts}}$$

where

- The term “All Conflict Alerts” is the sum of all conflict alerts which were identified.
- The term “Correct Alerts” the sum of all correctly identified conflict alerts.

The Detection Rate of conflicts is calculated as:

$$DR_{CD} = \frac{\sum \text{Correct Conflict Alerts}}{\sum \text{Real Conflicts}} \quad (10)$$

where

- The term “Correct Conflict Alerts” is the sum of all correctly identified conflict alerts.
- The term “Real Conflicts” refers to the number of really existing conflicts.

To evaluate the performance of the conflict detection module the previously described short simulation scenarios are used. Using the current setup of the system an alert is written to the database every five seconds. This is done repeatedly as long as the conflict exists. Therefore only the time of the first occurrence of a conflict has to be taken into account.

In order to gain the values for the term „Real Conflicts“ and the corresponding “Correct Conflict Alerts”, again a replay of the validation exercise run has to be inspected..

The conflict detection module of the SACom prototype has not been validated yet, as the progress in the project was not planned to reach this step already. The validation of the conflict detection module will be done in the near future. Nevertheless also the definition of a „conflict” is still in discussion.

7. CONCLUSIONS AND NEXT STEPS

The description presented herein only touches the detailed work needed to establish a full system validation, but may raise interest to look in further literature presented by the project participants.

Regarding the discussed ATM security prototype SACom the adherence to the developed methodology appears to be straightforward and clearly focuses on the development of tailor-made validation exercises.

This led to the described approach which shall validate the prototype as well module-wise as the prototype on the whole. The achieved values and insights are still subject for further improvement, although the presented first results encourage developing SACom further.

The quantitative findings described in chapter 6.2 will be enriched further when evaluated in combination with qualitative values achieved with questionnaires. These questionnaires need to be answered by the ATCos during and after the validation exercises.

One big challenge in the future of secure ATC voice communications will be, that existing speech data analysing tools (speaker verification, speech recognition) still need higher quality voice samples for evaluation than available in real air traffic voice communication. Another interesting result of the analysis so far is the challenge to handle female utterances with a speaker verification module. Female voices seem much more difficult to identify than male voices and it is much more difficult to distinguish between stressful and non-stressful utterances.

Regarding the near future the combination with other prototypes developed in the project is of high interest. Within these exercises the discussed single indicators of the SACom prototype will be correlated to one “global” indicator which will rate the overall situation in ATC voice communication taking into account a weighting of the different indicators. This correlated value will be automatically submitted (together with the single module indicators / scores) to the central element of the ATM Security Framework [1] but may also be transmitted to any other ATM security system.

It has to be said that research in the field of ATM security is still at its beginning. The way is paved by guidance of programmes like SESAR and NextGen, but the practical implementation and realisation is widely missing regarding ATM security issues. The lack of a commonly accepted validation methodology for ATM security prototypes, tools and systems shows that the community is in dire need of defining it. The security validation approach developed in GAMMA has the potential to be adopted to be the sought-after construction kit.

8. ACKNOWLEDGEMENT

The authors would like to thank all GAMMA consortium members that contributed to this paper through stimulating discussions around the concepts presented.

9. DISCLAIMER

The views expressed herein are the authors’ own and do not reflect a GAMMA consortium and/or their employers’ position or policy.

10. REFERENCES

[1] GAMMA Consortium, 2015, GAMMA CONOPS, The Ultimate ATM Security Framework, Newsletter, Issue No 1, pp. 2-3.

[2] International Civil Aviation Organization (ICAO), Annex 11 to the Convention on International Civil Aviation, “Air Traffic Services”, 13th Edition, July 2001

[3] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic, “On Perception and Reality in Wireless Air Traffic Communications Security”, Cornell University Library, eprint arXiv:1602.08777v2 [cs.CR], 2016.

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

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

[6] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, C. Neeteson, „Towards a more secure ATC Voice Communications System“,34th Digital Avionics Systems Conference, September 13-17, 2015.

[7] Result of AcListant-Trials in October 2014: H. Helmke et al. Assistant-Based Speech Recognition for ATM Applications, in: “Eleventh USA/ Europe Air Traffic Management Research and Development Seminar (ATM2015)”, Lisbon, Portugal, 2015.

[8] EUROCONTROL, 2010, European Operational Concept Validation Methodology, Version 3.0, https://www.eurocontrol.int/publications/european-operational-concept-validation-methodology-eocvm.

[9] P. Montefusco, R. Casar, T. H. Stelkens-Kobsch, R. Koelle, „Addressing Security in the ATM Environment“, ARES 2016, 11th International Conference on Availability, Reliability and Security, September 2016.

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

[11] T. H. Stelkens-Kobsch, M. Finke, D. Kolev, R. Koelle, R. Lahaije, „Towards Validating a Security Situation Management Capability“, 2016 Integrated Communications Navigation and Surveillance (ICNS) Conference, April 19-21, 2016.

11. EMAIL ADDRESSES

tim.stelkens-kobsch@dlr.de
michael.finke@dlr.de

2016 Deutscher Luft- und Raumfahrtkongress (DLRK)
September 13-15, 2016