# *Validating an ATM Security Prototype – First Results*

Tim Stelkens-Kobsch; Michael Finke, Matthias Kleinert, Meilin Schaper
Institute of Flight Guidance
German Aerospace Center (DLR)
Braunschweig, Germany
{tim.stelkens-kobsch, michael.finke, matthias.kleinert, meilin.schaper}@dlr.de

***Abstract*—Since years it is known that radio communication used by ATC can easily be intruded and is therefore subject to recurrent attacks. Nevertheless the voice communication between pilots and air traffic controllers is still the most flexible and efficient medium especially in a busy traffic environment, in non-standard situations or simply when exchanging air-ground messages in plain language is needed. As vulnerability seems not dominant compared to the number of crucial damages, voice communication is still the basic and most important communication method within the aeronautical mobile service. This motivated the development of a prototype called 'Secure ATC Communications' (SACom) within the frame of the Global ATM Security Management (GAMMA) Project. The paper at hand describes the required functionalities of the prototype, the validation approach taken, using this security prototype as example, and conclusions for the results of validation, regarding the prototype itself as well as the validation methodology applied to the security context within ATM.**

***Keywords—Security; ATM; voice communication; Global ATM Security Management Project; stress detection, conformance monitoring***

## I. Introduction

The challenge when designing a security management prototype for ATM is not only to find out if the concept is appropriate to minimize the expected impact of possible attacks. In fact the benefit for the participating stakeholders has to be evaluated and proven by appropriate evidence. The need for evidence leads to the understanding that there is a clear lack existing between the theoretically defined outlines by NextGen and Single European Sky ATM Research (SESAR) and the measures at hand to validate prototypes in the area of ATM security.

The paper highlights the approach to validate the proposed SACom prototype. Therefore the paper describes the intended functionality of the prototype and the different modules it consists of. Moreover the surrounding validation environment and the dedicated validation platform for investigating the prototype is elaborated and described in detail.

Within the GAMMA project [1] the SACom prototype is designed and developed. The verification of the prototype has been conducted in the Air Traffic Management Validation Center of the German Aerospace Center (DLR) in 2015 / 2016, whereas the first validation exercises were conducted in late spring of 2016.

The prototype will not only be verified and validated as a single system. Moreover, during the preparatory work for the validation exercises a small scale experimental setup was used together with partners in the project in order to elaborate added value of the presented prototype already as a pre-production sample.

The obtained results demonstrate the general feasibility of the developed prototype. A detailed discussion of the preliminary validation results will be done at the end of the paper.

This research-in-progress paper presents the initial findings from the validation and initial implementation of the security management prototype for secure ATC communications. The recent work supports the current security engineering needs and offers an iteratively deployable capability to complement the current ATM / CNS system and future deployment activities under SESAR or NextGen. The applied approach for the validation of this single prototype provides a mature basis for setting up a distinct methodology for validation of other ATM security oriented systems.

The next chapter explains the motivation behind the development of this ATM security prototype whereas chapter III explains the approach chosen for the development of the validation methodology. In chapter IV the validation approach is described exemplary with a tangible example. The following chapters V and VI present first results of the validation exercises and give an outlook to upcoming activities.

## II. Background

### *A. GAMMA Project Overview*

The GAMMA Project is one of the first European projects to address the growing importance of ATM security issues including new scenarios created by SESAR initiative. Besides identifying security threats and vulnerabilities, possible mitigation actions shall be investigated and validated. The role of all affected ATM stakeholders as well as regulatory aspects, standardization and human factors shall be considered. To achieve this, a bandwidth of highly experienced project partners from research institutes (e.g. the DLR), universities (e.g. the Slovak academy of sciences (SAV)), industrial partners (e.g. Airbus DS, Finmeccanica, Thales) and subject matter experts (e.g. ENAV, ROMATSA, 42 Solutions) cooperate in GAMMA. The project started in September 2013 and will continue until August 2017.

### B. *Recent Research Activities*

Within the GAMMA project, a comprehensive analysis of the existing ATM system and ongoing developments was performed to identify present and near future security risks in ATM. Based on SecRAM [2], security risks were investigated for typical primary aviation assets such as Communication, Navigation, Surveillance (CNS), information management and information exchange systems, airport facilities and avionics. Identified risks were categorized in the impact areas of personnel, capacity, performance, economy, branding, regulations and environment and assessed in terms of confidentiality, availability and integrity.

Based on this risk assessment, several innovative ATM security prototypes and / or threat detection prototypes are designed and developed for detecting / mitigating selected threats. In a newly defined ATM security architecture, developed prototypes are integrated in a data exchange network with a central node, the so called Security Management Platform (SMP), which is one of the prototypes developed within GAMMA. During the runtime of the GAMMA project the prototypes as well as parts of the developed security architecture will be validated.

### C. *Security Risk 'Air-Ground Voice Communication'*

The commonly used analogue voice communication between air traffic control and aircraft pilots is one of the major security risks identified within the GAMMA project. These radio transmissions are nowadays neither encrypted nor verified by a signature nor otherwise protected and can easily be intruded by unauthorized persons [3].

### D. *System to be Validated*

One of the prototypes is SACom developed by the DLR together with SAV, which addresses the security risk mentioned above. Preconditions set before developing the system are the following:

The system shall be developed as a threat detection system,

The system must not interfere with the existing ATC or cockpit equipment to maintain the current level of safety,

The system must not in any way influence or endanger the work of pilots or controllers,

Detection functions shall be based on monitoring the voice communication and the actual traffic situation only.

Due to these constraints, it was decided to choose a modular system design, containing the following functions:

1) The system shall identify unauthorized speakers in analogue air-ground communication,

2) The system shall identify mental pressure of the person intruding into the analogue air-ground communication,

3) The system shall identify aircraft deviating from the cleared flight route or the cleared level (due to a possible false command by an unauthorized person),

4) The system shall identify safety-critical ATC clearances issued by the air traffic controller (ATCO),

5) The system shall correlate these individual indicators and send an alert to the Security Management Platform (SMP).

Enumerated points 1) and 2) are solved by means of voice pattern analysis methods developed by SAV [4]. For speaker verification purposes, all persons who shall be recognized as authorized persons must be introduced to the application with a so called voice enrollment.

Enumerated points 3) and 4) are solved by means of conformance monitoring methods [5]. Originally, these algorithms were designed to detect safety problems (navigational failure, non-compliance due to human errors etc.) and were not used in the frame of ATM security before. However, these functions described in 3) and 4) require also information about the given ATC clearance in real time. As just the monitoring of voice communication and the traffic situation is allowed, speech recognition technology developed by DLR in a former project (AcListant) is used [6].

Enumerated point 5) is solved by calculating an overall threat indicator score considering the single indicators from the detection modules of the prototype together with weighting factors, defined alert thresholds and module reliability within a certain time frame. One hypothesis is that single indicators do not distinguish between a safety and a security problem, but multiple indicators at the same time may indicate a security threat.

Primarily, SACom shall act as a threat detector to immediately and automatically send alerts to the SMP. With this automatism persons responsible for security related decision making or management of security get the information immediately. Nowadays, this chain of reporting mostly relies on face-to-face or phone coordination, which takes some time until information are passed through and due to the large number of chain links there is a risk of loss of information.

Secondarily, in order to enable the persons directly confronted with and in charge of handling the security threat tactically, it was also decided to investigate the benefit of direct presentation of the system output on suitable Human Machine Interfaces (HMIs) in the cockpit or in the controller working position (CWP).

## III. Validation Methodology

When planning validation work the first decision is to choose the most appropriate methodology. Within GAMMA the choice was either to follow the European Operational Concept Validation Methodology (E-OCVM) [7][8] or the Open Source Security Testing Methodology Manual (OSSTMM) [9]. Regarding the strong connection of ATM with the project at hand the E-OCVM was identified as the validation methodology to be applied. This results from the fact that OSTMM is more cyber security oriented, whereas E-OCVM was especially invented for application in validations regarding ATM.

As the E-OCVM states, validation is a generic term with many meanings [7]. Validation is seen as an iterative process by which the adequacy of a new system or operational concept being developed is established. The E-OCVM focuses on providing evidence that the concept is “fit for purpose” and answers the question, “Are we building the right system?”.

The validation approach depends on the maturity of the concept to be validated and the corresponding V-phase in the lifecycle. The validation activities necessary in the different V-phases are depicted in Figure 1.

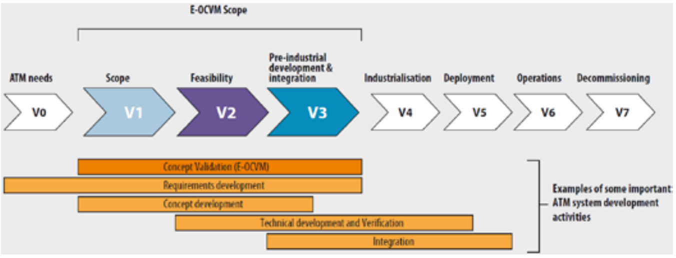
E-OCVM Scope
ATM needs
Scope
Feasibility
Pre-industrial development & integration
Industrialisation
Deployment
Operations
Decommissioning
V0
V1
V2
V3
V4
V5
V6
V7
Concept Validation (E-OCVM)
Requirements development
Concept development
Technical development and Verification
Integration
Examples of some important ATM system development activities

Figure 1: Lifecycle V-Phases [7]

After the concept is developed it will be validated and improved during the phases V1 to V3. The validation checks, if the concept describes the “right system”. The technical development, which starts in phase V2 is based on that concept. The verification checks if the developed systems corresponds to the developed concept and ensures that “we are building the system right”.

E-OCVM has proven its applicability in many different use cases and is widely used for validation purposes. However, it is sometimes needed to adjust the procedure slightly in order to consider experiences already made. The strategy applied for validating the described SACom prototype is therefore a combination of this well-accepted European standard and best practice.

### A. *Validation Goals*

When applying the methodology, one of the first actions is the identification of validation goals. These goals have to be based on stakeholders’ needs. The definition of validation goals furthermore has to be aligned with the global project objectives defined in advance. Then the compliance of the set of objectives can be assessed.

When talking about validation goals it is helpful to distinguish between goals which can be applied over the entire scope of the topic (global validation goals) and a set of more specific goals considering the validation strategy. The strategy related validation goals may be further subdivided in three parts:

- Goals focused on validation of individual tools,
- Goals focused on partial integration of tools and
- Goals focused on full integration of tools with the environment

### B. *Validation Objectives*

Validation objectives are more specific than validation goals. They can be reached by specific actions and support the attainment of the associated goal. Objectives must be measureable and tangible. The validation objectives for a project should be set as part of the project planning process and will then be decomposed and linked through definition of the work plan and the individual exercise plans.

Validation objectives “determine the scope, direction and design of the validation activity” (see [8], p. 31). In order to define the validation objectives questions like the following should be answered [7][8]:

- What is the aim of the validation process during each V-phase of the Concept Lifecycle Model?
- What can be realistically achieved in the validation process during each V-phase?
- What do stakeholders expect from validation during each V-phase?
- What would be an acceptable output at the end of each V-phase?
- What specifically will validation address?
- What are the transition criteria for the concept(s) or concept elements to progress to the next V-phase?

### C. *Key Performance Areas*

Key performance areas (KPAs) are broad categories that describe different areas of performance of an ATM system; they are “a way of categorizing performance subjects related to high-level ambitions and expectations” [10]. The performance framework published by ICAO has 11 categories: safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, interoperability (see [7]). The defined key performance areas offer starting points for hypotheses and for defining key performance indicators. It may be the case that not all of the mentioned key performance areas may be applicable to the specific system under validation.

### D. *Key Performance Indicators*

Key performance indicators (KPIs) measure performance in key performance areas and are identified once the key performance areas are known. A key performance indicator is a measure of some aspect of a concept or concept element, for example, “the total number of runway incursions per year”, “mean arrival delay per week at airport X” [7].

### E. *Validation Requirements*

Ingredients for the definition of validation requirements are on one hand the validation goals and objectives identified and on the other hand the KPA and KPI [7][8].

Validation requirements are needed to identify necessities and enablers for the validation activities. Formulated requirements are a measuring rod to assess validation results. Requirements could be e.g. the timely availability of a performance framework, availability of suitable modeling tools, platforms, reference data etc. [7].

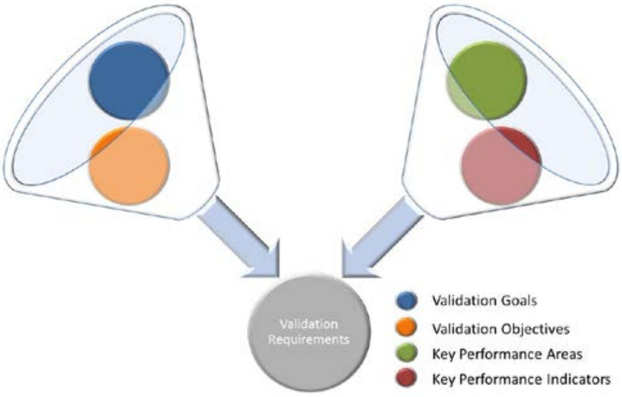

Figure 2: Composition of validation requirements

In order to achieve the validation requirements the first and very critical task is to identify how the validation objectives will be assessed in general terms (e.g. validation infrastructure available, policies). Furthermore it has to be identified how the project will conduct its validation activities (i.e. which validation tools and techniques will be applied to which aspects of the problem). The elaborated validation requirements have to be refined repeatedly during the process. This means that more detail has to be added to the exercise environment defined by the project and to the applied methods each time new results from the validations are available. The assumptions made throughout this process should be recorded.

Within the project driving this paper another differentiation has been done. For each planned validation exercise the validation requirements have been declared as

- Validation environment requirements:
  Requirements related to all assets, so called validation environment building blocks (VEBBs), needed to perform the validation exercise such as simulators, emulators etc.

- Prototype requirements:
  Requirements related to the prototype functionalities, derived from the GAMMA concept.

- Validation platform system requirements:
  Requirements related to the integrated setup of the prototype(s) connected with the VEBB(s).

The above indeed always has to be adjusted to the specific application area of the prototype. The main issue at this stage of a validation is to show that the prototype is seen as beneficial; the involved stakeholders trust the advice derived from the newly designed systems and they are enabled to isolate, avoid or resolve the security problem.

## IV. Validation Approach for SACom

Within this and the following chapters, the methodology described above is further specified for the proposed SACom prototype. The steps are elaborated one by one for the specific development. This fosters the contribution of the prototype to a more secure ATC management.

### *A. Validation Goals, Objectives, Key Performance Areas, Key Performance Indicators for SACom Validation*

The following validation goals were defined for the SACom prototype [11]:

- The proposed prototype contributes in a beneficial way to the overall security management process.
- The information is available at the right place at the right time.
- Sensible information is only available for authorized roles.
- The information displayed to the user is considered usable, useful and beneficial.
- The detection of unauthorized participants in air-ground-communication is improved compared to a situation without the system.
- The system and related procedures can be implemented and used safely in the existing ATM.
- The performance of the SACom prototype is acceptable (regarding false alarms, correct detection, usefulness and trust).
- The SACom prototype leads to a better situational awareness of the ATCO as well as pilots regarding unauthorized intrusions into air-ground voice communication.

With reference to the KPA defined by ICAO the following subset of KPA has been identified as applicable for the validation of the SACom prototype:

- Safety,
- Security,
- Capacity,
- Predictability.

Further, the following key performance indicators were defined for the SACom prototype:

- False alarm rate (Safety),
- Detection rate (Security),
- Number of detected dangerous / undesired aircraft behavior events in a defined time frame (Safety, Security, Capacity, Predictability),
- Recorded time until detection (Safety, Security, Capacity, Predictability),
- Number of unauthorized speakers detected in a defined time frame (Security).

### *B. Validation Requirements for SACom*

For the SACom validation exercise, the following validation environment requirements have been defined [12]:

- The validation environment shall provide a controller working position including all tools and assistance systems needed for the safe conduction of air traffic control according to present standards.
- A voice communication system simulating the air-ground voice communication shall be in place, which

is equal in its handling to existing ATC radio communication equipment.

- Pseudo pilot stations shall be in place, allowing a realistic simulation of the pilot-controller interaction assuring realistic aircraft behavior and reactions.
- The validation environment shall allow real-time validation.
- Gathered data such as voice communication, prototype inputs and outputs as well as relevant events simulated during the exercise shall be recorded.
- Wherever a self-assessment or direct information from the test person is required, the validation environment shall allow him or her to state and record this information.

Further, the following prototype requirements have been defined before the development of the system [13]:

- The SACom prototype shall monitor the air-ground voice communication in real time and verify the authorization of all speakers by means of voice recognition.
- The SACom prototype shall monitor the air-ground voice communication in real time and detect voice patterns in the transmissions of all speakers which are typical for stressful situations.
- The SACom prototype shall provide means to monitor the compliance of all aircraft under responsibility of the ATCO to given clearances.
- The SACom prototype shall provide means to check if given ATC clearances do not induce safety-critical situations such as conflicts between two aircraft.
- The SACom prototype shall correlate all of the above mentioned indicators and provide status reports and alert messages, which are supposed to be sent to the SMP in live configuration.

The following validation platform system requirements have been defined [14]:

- The interfaces between the SACom prototype and the validation environment building blocks shall use standard data formats (such as wav format for audio data or Asterix Cat 62 for radar data).
- Status reports of the SACom prototype shall be transmitted via a defined interface which is similar to the one used in live configuration with the same format / protocol.

### C. *Design of SACom Validation Trials*

The validations for the GAMMA project and its prototypes started in April 2016 and are planned to be conducted until August 2017. Within this period, several validation trials will be performed at intervals of approximately 3-4 weeks. The idea behind is to gather experience, work on troubleshooting and to implement a continuous process of optimizing the prototype until the final validation trials take place.

ATCO-centric exercises are performed as sets of Human-in-the-loop real-time ATC simulations for the SACom prototype. Underlying ATC environment is the simulated approach control sector of Düsseldorf Airport in Germany, the traffic scenario contains a usual number of Instrumental Flight Rules (IFR) arrivals in a defined time period and stable weather conditions. All aircraft are steered by two or three trained pseudo pilots in an n-to-m relationship. Voice communication will be simulated with a Voice over IP (VoIP) radio communication simulator. The role of the ATCO will be performed by an external ATC expert as test person; whenever possible an active ATCO. The SACom prototype will be installed at the CWP. The focus lies on all aspects of ATC work with a high level of realism. Such an exercise takes about one day and consists of the following parts:

- Briefing of all exercise participants, especially the test person acting as ATCO taking part in the simulation.
- Voice enrollment for speaker verification.
- Simulator training to make the test person familiar with the used simulator equipment and configuration.
- A number of short simulation runs with pre-defined scenarios containing single events related to the identified security threat or to safety events with similar effects. These events always involve any type of non-compliance of one or two aircraft which leads to a loss of separation if not solved (e.g. wrong execution of an ATC clearance, no execution of an ATC clearance, performing any manoeuver without an ATC clearance). Reasons for these events may be simulated pilot errors, simulated technical failures or simulated fake instructions by an unauthorized third person taking part in radio communication. In these simulation runs, the prototype will already be active but there will be no indications to the test person.
- Prototype training to make the test person familiar with the SACom system and its indications.
- A final simulation providing the threat scenario of unlawful intrusion into air-ground voice communication. This threat was also identified by the risk assessment of the GAMMA project. Here the test person shall try to continue the work as long as possible using tactical countermeasures while maintaining safety and, if possible, keep the sector capacity,
- Debriefing and questionnaire.

### D. *Measurements and Data Gathering*

As described above, this exercise contains short simulation runs as well as long simulation runs of a different nature, therefore different values and features are measured / assessed accordingly.

For the short simulation runs, the following indicators are determined:

- Sum of predefined events successfully simulated during all short simulation runs.
- Sum of events correctly detected by the prototype during all short simulation runs.

- Sum of events correctly detected by the air traffic controller during all short simulation runs.
- Sum of false detections by the prototype during all short simulation runs.
- Sum of false detections by the air traffic controller during all short simulation runs.
- Time until the event is correctly detected by the prototype.
- Time until the event is correctly detected by the air traffic controller.
- Correlated threat indicator of the prototype for each event.

For the long simulation run, the following indicators are determined:

- Number and type of non-compliant actions induced by the intruder.
- Related tactical countermeasures used by controller.
- Time period from the insertion of fake comments until a safe, orderly and fluid flow of traffic is recovered.
- Number of correctly verified speakers.
- Number of correctly detected unauthorized transmissions.
- Number of false detections.
- Number of missed unauthorized transmissions.
- Matching values for all transmissions of the speaker verification.
- Stress detection values for all transmissions.
- Correlated threat indicator of the prototype as a function of time.
- Acceptance assessment by means of a questionnaire.

## V. First Results and Discussion

In the following chapter, the first results of the validation activities using the setup and procedure described above are presented and discussed. On one hand the focus lies on the results of the prototype validation itself, on the other hand the experiences made with this validation procedure are discussed.

### *A. Speaker Verification*

The validation activities showed, that match values of 90 percent or more are possible and where occasionally achieved for speaker verification by automatic voice analysis. This match value is a result from the comparison of the analyzed audio stream with a pre-recorded voice example of the authorized speaker (the so called ‘enrollment’).

The quality of the analyzed audio stream plays an important role; little background noise, minor distortions, overamplification or changing audio equipment and microphones already have a significant impact on the matching value.

Additionally, the stress level of the speakers has a direct influence on the result as some voice characteristics change in high-stress situations, such as the pitch of the voice, the speech velocity and the articulation. Therefore it exists a direct dependence between speaker verification and stress detection.

The speaker verification function as it was implemented for first validations needed a continuous audio stream of at least three seconds to produce reliable results, which also means that the result is available just after this time period has passed (and not earlier). Hence, for the setup used, the results were usually displayed shortly after the end of each transmission.

In a busy traffic situation, the controller-pilot communication has shown a dense sequence of rapidly spoken short transmissions. Therefore some transmissions are shorter than the minimum required time period for analysis and cannot be analyzed. This fact causes problems in correctly separating the audio transmissions again, which hinders the preparation of the speaker verification analysis. A successful speaker verification analysis needs successful differentiation of each distinct transmission, because it must be made sure that each speaker transmission is analyzed separately. If this is not assured it is sometimes very difficult for the controller to maintain the awareness about which result belongs to which transmission.

Further, depending on the traffic load, the controller sometimes does not have enough time to carefully monitor the speaker verification results.

### *B. Stress Detection*

During the validation activities, an increased stress score could hardly be detected in a reliable way due to the following reasons:

- Controllers seem to be very used to stressful situations and they are trained not to show their stress.
- Due to the simulation, the experienced stress level is significantly lower than it would be in a real situation.
- Attempts to detect stress of the unauthorized speaker fail, because the intruder (who indeed acts his role) does not show stress at all and up to now no possibilities have been identified to induce stress.
- With the applied measures and means it is impossible to reliably distinguish between stress caused by unlawful interference and stress caused by a high workload, unfamiliarity with the used systems etc.

### *C. Conformance monitoring*

In the scope of this project, conformance monitoring is used to detect unusual aircraft behavior. Unusual means in this case that an aircraft is somehow deviating from the clearances instructed by an ATCO. Those deviations are used as an indicator that maybe an unauthorized person (false ATCO) is giving fake clearances to the pilots. In order to identify deviations, the system needs to know the clearances instructed by the authorized ATCO (i.e. the clearances have to be fed into the system). This can be done in different ways. One approach is to monitor the mouse and keyboard and force the ATCO to enter every clearance manually into the system. Another approach is to use speech recognition on the ATCOs side to automatically recognize the commands and feed them into the System. This limits the ATCOs additional work to those commands that were not correctly recognized by the system.

The validation activities show that the mouse / keyboard approach is not feasible under normal working conditions. In order to give a proper support regarding conformance monitoring, the system needs to be aware of every clearance concerning speed, flight level and direction shortly after it is instructed. Especially in high traffic situations the time difference between giving the clearance to a pilot and entering the command into the system gets too big or, even worse, the ATCO tends to omit entering some commands into the system.

The validation activities also show that the benefit of conformance monitoring for the ATCO highly depends on the current situation. During low or normal traffic conditions the ATCO usually detects most of the deviations almost in the same time as the system does. But especially under high traffic conditions or times of lower awareness the system tends to be a lot faster than the ATCO. Furthermore deviations are much better recognized by the ATCO when he is alerted and is expecting anything unusual happening. One test person for example was completely surprised about the deviations during the first short simulation runs and it took a relatively long time until he recognized the deviation. After the 3rd short simulation run he was highly alerted, which prompted him to expect a deviation of any aircraft, to monitor the aircraft more closely and to set the focus not so much on an expeditious and economic planning of the traffic but more on planning and guiding the traffic in a safe way maintaining a higher separation between aircraft. This means that, due to this pro-active countermeasure, aircraft deviations do not immediately cause a safety-critical situation when they act not conformant.

Another effect, which could be confirmed especially during the long simulation run, is the "time until the event is detected" as a critical factor which has a direct influence on the workload of the controller. The more time was needed to recognize the deviation, the more work effort was necessary to bring the considered aircraft back on track.

The most critical deviations are flight level deviations, as the ATCO has to recognize the aircraft flight level in the radar label and process this information in the mental traffic picture. Lateral deviations can instead directly be recognized on the radar screen and are directly visible as lateral deviation of the aircraft target. Speed deviations need a long time to cause any conflict between two aircraft and can be seen as the least critical type of deviation.

### D. *Correlation and reporting to the SMP*

The SACom prototype looks at the different information generated by speaker verification, stress detection and conformance monitoring. Based on this information different types of alerts are reported to the SMP.

- Speaker Verification Alert – Unauthorized speaker detected in one transmission.
- Stress Detection Alert – High stress level detected in one transmission.
- Conformance Monitoring Alert – Deviation between ATCO clearance and aircraft behavior detected
- Conflict Detection Alert – Two aircraft are cleared for a flight route that will result in a collision or infringement of separation.
- Correlated Alert – Correlation of all alerts over a defined time window combined with weighting factors. If the correlated value reaches a defined threshold the alarm is triggered.

The significance of a correlated alert of course mainly depends on the weighting factors, the time window and the alert threshold chosen. Those variables are different for every ATC-unit and influenced by different factors:

- Mode of operation in the respective sector.
- Local characteristics of the airspace.
- Current traffic load.
- Reliability of the different modules (Speaker Verification, Conformance Monitoring etc.).

All those factors still have to be determined in order to set the right values for the different variables. But even when all the variables are set to appropriate values, an alert reliability of one hundred percent is not possible. Therefore the settings of the variables will always be a tradeoff between fast security alerts with lower reliability or slower security alerts with high reliability.

The validation activities show that during a simulation run with different attacks and threats, a lot of messages are generated and sent to the SMP. To handle all those messages without assistance systems would be too much for a human operator. The SMP instead will put all these information into the right context and alert the responsible operator only if necessary.

### E. *Conclusion – SACom prototype*

Regarding the speaker verification function, the following conclusions can be drawn from the results described above and experiences gained during the first validations:

- The robustness against a reduced audio quality must be improved significantly; especially when used for security reasons, where a very high reliability of the result is mandatory.
- Due to the unavoidable time span from the beginning of the transmission until the voice of the speaker is verified, the direct blocking of unauthorized transmissions or any other direct mitigation action is impossible. Following this, the system cannot be used to prevent the intrusion into the air-ground voice communication.
- Time delay from the beginning of the transmission until availability of final analysis must be shortened; if possible the result should already be available before the end of the transmission under analysis.
- Speaker verification results are only of minor usability if displayed at the controller working position; just alerts should be indicated.

- As the pilot is the person who is directly confronted with possible fake clearances from an unauthorized person, the speaker verification application may be more beneficial when available on the pilot side (i.e. aircraft cockpit).
- The speaker verification matching values are in principle meaningful enough to enable the pilot to distinguish between unauthorized and authorized transmissions. This indeed requires a continuously high reliability and accuracy of the analysis result; otherwise a significant safety risk could be introduced.

Apart from these findings and conclusions, also the following points have to be solved:

- The speaker verification as it is implemented during these trials requires an efficient enrollment management as there must be an enrollment for every controller and every pilot who may be involved in controller-pilot voice communication.
- The system can easily be defeated by using recorded data from live ATC communication for the intrusion.
- The system will not detect an unlawful intrusion by a person who owns a valid enrollment and is listed as authorized speaker.

Regarding the stress detection function, the following conclusions can be drawn from the results described above:

- The theory behind the stress detection is very complex and is still fundamental research. There is absolutely no experience for detecting stress patterns in the controller-pilot voice communication [15], and due to the large variety of stress-inducing factors (workload, safety issues, security issues, etc.), further research activities as well as the method of analysis must be more specific to the ATM context;
- A simulation environment is not fully suitable to validate stress detection. Real audio recordings or shadow-mode techniques should be used instead. In parallel, it needs to be investigated if and how persons executing unlawful actions show any kind of stress.

Apart from these findings and conclusions, it has to be considered that stress can also be a natural phenomenon in aviation (emergency situations, training situations) and is inappropriate as an indicator for security problems.

For the conformance monitoring function, the following conclusions can be drawn from the results described above:

- The system needs an input methodology that ensures a fast and reliable input of every ATCO clearance.
- The use of conformance monitoring methods in combination with speech recognition of the ATC clearance proved as best suitable for this purpose and has the potential to be a very powerful instrument to quickly detect aircraft deviating from the instructed flight path (provided that the ATC clearance recognition rate is satisfying).
- Conformance monitoring alone is not an appropriate indicator for detecting an unauthorized speaker issuing fake clearances, as deviations can have different reasons (e.g. pilot action without clearance, wrong pilot action etc.); conformance monitoring does not distinguish between deviations caused by safety issues and those caused by security issues.
- Therefore there are rather safety benefits than security benefits as flight path deviations are typical for both, but safety reasons are much more likely.
- Highlighting the identified deviations in the corresponding radar can increase safety especially in high traffic load situations. Depending on the ATCOs awareness and workload it shortens the reaction time and helps to prevent after-effects.
- In order not to overload the radar display with deviation warnings, a filtering algorithm shall be in place which presents just the most urgent warnings.
- Deviation tolerances should be very strict for deviations from flight level, less strict for lateral deviations and may be quite generous for speed deviations, depending on the local needs.

### *F. Conclusion – Validation methodology*

When looking at the distinct steps undertaken for the development of the SACom prototype one may derive a blueprint for defining the needed requirements for validating as well security management prototypes as parts of security management architecture.

With this paper the approach to validate the prototype SACom is described in detail and the results pave the way for possible refinements of the presented methodology in parts. On the other hand the appropriateness of the developed validation methodology is proven and facilitated.

As security in ATM is not clearly separated from flight safety, it should always be investigated if the system which is subject for validation has also positive or negative effects on safety, capacity or other key performance areas of the whole ATM environment (e.g. capacity). Therefore the role of a prototype provided for the ATM system must be clearly described before the validation exercises start. Especially for the assessment of human factors affecting the work with the newly invented system, an involvement of ATM experts and experienced ATM operators is very important.

During the development of an ATM security prototype it is almost impossible to define all system requirements in the first attempt; especially some requirements derived from integration into the existing or near future ATM processes cannot be recognized until the validation activities start. Especially factors like information flow, information display and system speed requirements need to be monitored and adjusted regularly during the development process.

Especially for security (prototype) validation using real-time human-in-the-loop simulation, at least 10% of all planned security events cannot successfully be simulated because it cannot always be predicted how the simulation (i.e. the traffic situation) will develop. Each ATCO works in a slightly different way, which results in considerable different traffic situations after some time.

Regarding involved test persons, it is a big challenge to avoid expectations regarding the validations on their side. If somebody expects simulated security threats it is difficult to keep the shock effect comparable to real life. This sums up with the usual difficulties of human-in-the-loop simulations like training effects during the exercises. In real life, security events do almost never involve a pre-notification and shock effects may be essential for the success of such events. For validation purposes, one of the main goals is to reproduce these shock effects as realistic as possible.

## VI. Outlook and further activities

As the validation activities have just started, the work will continue and more findings, adjustments or the introduction of additional validation tests can be expected on the way to the proof-of-concept of this prototype as standalone-system.

In the later part of the GAMMA validation phase, the SACom prototype will be validated also in combination with other GAMMA prototypes interconnected in a network. This opens plenty of possibilities for automatic analysis and correlation and prediction algorithms inside of the envisaged Security Management Platform.

Nevertheless a lot of further necessary research work has already been identified, which cannot be covered within the GAMMA project. These items can be found especially

- In the stress detection area regarding voice patterns and its validation; this applies in general, in aviation and specifically in an ATC environment.
- In analyzing low quality voice signals similar to current ATC-pilot radio communication including background noise for the purpose of speaker verification.
- In tweaking the voice analysis to obtain results simultaneously to transmissions.
- In assembling with additional state of the art or future monitoring / alerting functions to improve correlation results.
- In creating, managing, updating as well as continuously activating and deactivating a large number of speaker enrollments worldwide.

## VII. Acknowledgment

The research leading to the results presented in this paper has received funding from the European Union FP7 under grant agreement no 312382.

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

## VIII. References

[1] www.gamma-project.eu

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

[3] 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 (DASC), Prague, September 2015.

[4] M. Rusko, M. Trnka, “Stress, Arousal and Stress Detector trained on acted Speech Database”, 18th International Conference on Speech and Computer (SPECOM), Budapest, Hungary, August 2016, in press

[5] T. G. Reynolds, R. John Hansman, “Conformance monitoring approaches in current and future air traffic control environments, 21st Digital Avionics Systems Conference (DASC), Irvine, CA, October 2002.

[6] H. Helmke, J. Rataj, T. Mühlhausen, O. Ohneiser, H. Ehr, M. Kleinert, Y. Oualil, M. Schulder, D. Klakow, „Assistant-Based Speech Recognition for ATM Applications“, 11th FAA/EUROCONTROL ATM-seminar, Lissabon, Portugal, June 2015.

[7] Eurocontrol (2010): E-OCVM Version 3.0 Volume I. European Operational Concept Validation Methodology.

[8] Eurocontrol (2010): E-OCVM Version 3.0 Volume II. European Operational Concept Validation Methodology.

[9] ISECOM (2010): OSSTMM 3. The Open Source Security Testing Methodology Manual.

[10] ICAO, “Manual on Global Performance of the Air Navigation System: Part I & II”, Doc 9883, edition 1.0, February 2008.

[11] GAMMA Consortium, Deliverable D5.1 “Validation Exercise Plan”, August 2015.

[12] GAMMA Consortium, Deliverable 7.2“Validation Environment design and development” 1st release, March 2016.

[13] GAMMA Consortium, Deliverable 6.2 “Prototypes Requirements”, October 2015.

[14] GAMMA Consortium, Deliverable 5.2 “Validation Platform System Requirements”, August 2015.

[15] M. Rusko, M. Trnka, “Stress, Arousal and Stress Detector trained on acted Speech Database”, 18th International Conference on Speech and Computer (SPECOM), Budapest, Hungary, August 2016, in press