USING SIMULATIONS TO VALIDATE SECURITY PROTOTYPES IN ATM

T. H. Stelkens-Kobsch, M. Finke
Deutsches Zentrum für Luft und Raumfahrt – Institut für Flugführung,
Lilienthalplatz 7, 38108 Braunschweig, Germany

Abstract

Simulations used for validation tasks provide a reliable means to evaluate the applicability and suitability of new procedures, processes and systems. The area of application spans from simple software simulations of isolated system functionalities over more complex simulations of whole processes and systems to human in the loop simulations of complete system of systems. This applies for nearly all areas of life and several methodologies have already been developed to standardize the validation approach. For air traffic management research this is also true and with the European Operational Validation Methodology a powerful and widely applicable list of measures is available. Following the developments and experiences of the past the above is valid despite for security related applications and processes.

Security in Air Traffic Management is an ever emerging topic, which is not only paramount since the attacks of 9/11/2001. In recent years there have been a lot of incidents caused by accidental, deliberate or even malicious actions. Within the Single European Sky Research Air Traffic Management Research Program and comparable programs the security aspect and especially the validation of security concepts and prototypes was of low visibility if not absent until today. Just in the shorter history this topic gains more and more interest, which is proven by several task forces and ad hoc working groups dealing with security issues in Air Traffic Management.

Applying human in the loop simulations to validate security prototypes is therefore a new challenge in validations. To achieve meaningful results the Institute of Flight Guidance of the German Aerospace Center developed new strategies, because the impact and success of security events depends a lot on the expectations of the exercise participant. In order to create a realistic simulation environment and an intuitive reaction, interfering training effects must be avoided by all means to keep the surprise effect within these simulation campaigns. Recent security-related simulations have been conducted within the Air Traffic Validation Center of the German Aerospace Center, which provides a complete setup for simulated radar control amongst others.

The approach to the experimental work started with the application of risk assessment and treatment methodologies, which however will be explained just briefly. The next steps were to identify suitable security controls to setup a tailor made prototype for the security research question at hand. Furthermore a dedicated simulation environment for the validations had to be provided. A parallel task was the transformation of identified security threats to a storyline of the conceived attacks. This storyline is used as a stencil for defining the scenarios and the subsequent conduction of the single prototype validations.

The paper will finish with conclusions about the simulation approach and discuss the relevance for the dedicated application area. [1]

1. INTRODUCTION

Validation and validation-like activities are found in a number of industries, which may be regulated and unregulated. Banking, aviation, software, microelectronics, nuclear power and others all incorporate practices closely resembling validation methods.

Validation activities in the aviation domain were of growing importance almost since the beginning of aviation itself. Initially validations were merely dedicated to questions of airworthiness of aircraft and certificates [1]. Over the years the application of validation activities was spread also to engineering design techniques and system concepts [2].

Since some years the European Operational Validation Methodology (E-OCVM) [3] is established as some kind of a standard for validation activities within aviation in Europe. This methodology is in line with the Operational Concept Validation Strategy Document (OCVSD) [4] widely used and accepted in the US.

Since their invention the validation methodologies have been applied for a wide variety of systems and concepts

[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.

in the aviation safety domain. This supported e.g. the establishment of safety management systems (SMS) as described in [5].

Having said this it is apparent that the above is not true for the security domain in the same manner. Looking at security there is few to nothing applicable when it would come to validation. The two main research programs in Air Traffic Management (ATM), the Single European Sky ATM Research (SESAR) [6] as well as the Next Generation Air Transportation System (NextGen) [7] are not providing tools, process descriptions or methodologies to validate security prototypes, concepts or procedures. To fill this gap the Global ATM Security Management Project (GAMMA) started in 2013.

Within GAMMA a concept for securing ATM should be developed accompanied by the design and building of seven different prototypes for a holistic security management [8]. Another and particularly important goal of the project was to validate the security prototypes based on the adaption of existing validation methodologies. In order to achieve this, a catalogue of suitable validation approaches needed to be established.

2. INITIAL STEPS TOWARDS SECURITY VALIDATIONS

What is still missing is a methodology to validate prototypes and concepts in the security context. It is therefore needed to make the expected benefit tangible and to validate the system ("are we building the right system" [3]). It is not sufficient to verify if the system was built right. The question is: are the newly introduced systems and functions (respectively processes) worth implementing?

To prove this question dedicated means need to be utilized which support a successful validation. The first decision is typically, if the experiments are suitable for a real life application or if a simulated situation shall be established. When this decision needs to be taken with respect to security related problems it is obvious, that real life attacks are not feasible (especially when thinking of validations with participation of humans).

Therefore it is recommended to set up simulations which nevertheless should be as realistic as possible in order to achieve results which are relevant also for real life. This leads to the next decision, literally the differentiation between

- Model based simulations including fast time simulations or
- Real time simulations including shadow-mode trials.

Within the project where the presented work originates from, security prototypes were postulated consisting of concepts for securing parts of the ATM system and taking human operators as the final authority for decisions. This means the prototype's results need to be presented to the operator by means of a Human Machine Interface (HMI).

When evaluating prototypes with mandatory human interaction for triggering next procedural steps this interaction also has to be accounted for in the experiments. This leads to Human In The Loop (HITL) simulations, where a human is part of the validation setup.

HITL simulations have already widely been used in respect to safety issues and evaluations but experience regarding validation of security questions by applying HITL simulations tends to zero. There are indeed simulations and validations taking human interaction into account but not in the ATM security domain.

3. RISK ASSESSMENT, RISK TREATMENT AND VALIDATION SETUP

The procedure to find the best suited kind of validation is one task. Designing the prototypes and/or controls which shall be validated is then another task. In the aviation domain one of the recommended methodologies is the SESAR Security Assessment Methodology (SecRAM) [9] to identify the needed controls which will lead to new systems that will enhance security and which are then validated. Within the course of GAMMA SecRAM was applied and a lack in security regarding VHF (Very High Frequency) voice communication was identified [10].

The additional security control which was developed as a result of applying this strategy is the so called Secure ATC Communication (SACom) prototype. The SACom prototype is a system designed and developed within the GAMMA project as a local detection system. Its purpose is to secure the air-ground voice communication between air traffic controllers and pilots, which is still done by using analogue radio transceivers and which is vulnerable against unauthorized intrusion, jamming or eavesdropping. The specific threat of an unauthorized person imitating the air traffic control service and giving fake ATC clearances to pilots is addressed by this system.

The SACom prototype has a modular architecture which is described in the following:

- Speaker Verification Module: This module continuously monitors the air-ground voice communication between pilots and ATC, isolates the individual messages that were transmitted on this frequency and cross-checks the voice characteristics of the spoken phrases with a database of known authorized speakers.
- Stress Detection Module: Similar to the Speaker Verification Module, this SACom component continuously monitors the air-ground voice communication between pilots and ATC to detect any kind of mental stress which is reflected in known voice anomalies such as arousal, pitch of the voice and others.
- Conformance Monitoring Module: This module uses surveillance data, flight plan data and recorded ATC clearances that were instructed by the air traffic controller. This is done on one hand to detect deviations from the current ATC clearance of any aircraft; more specifically lateral deviations, level deviations as well as deviations from the instructed speed. On the other hand the aircraft state vectors, the overall intention of the flight according to the flight plan and the latest ATC clearance is used to predict aircraft trajectories. These are in turn used to detect

possible conflicts between two aircraft, which may be caused by aircraft deviations or fake ATC clearances.

- Security Management Interface: This component collects all the different indicators and correlates them to an overall threat indicator score (>0). This correlated score, if applied in combination with a pre-defined alert threshold, can be used as the basis for automatic reporting of security-relevant information to a defined security management entity, e.g. the Security Management Platform (SMP), which is another prototype developed within GAMMA.

The following figure displays the overall SACom architecture including inputs and outputs. Further and more detailed information about the prototype and the security threats which are addressed by this system can be found in [11].

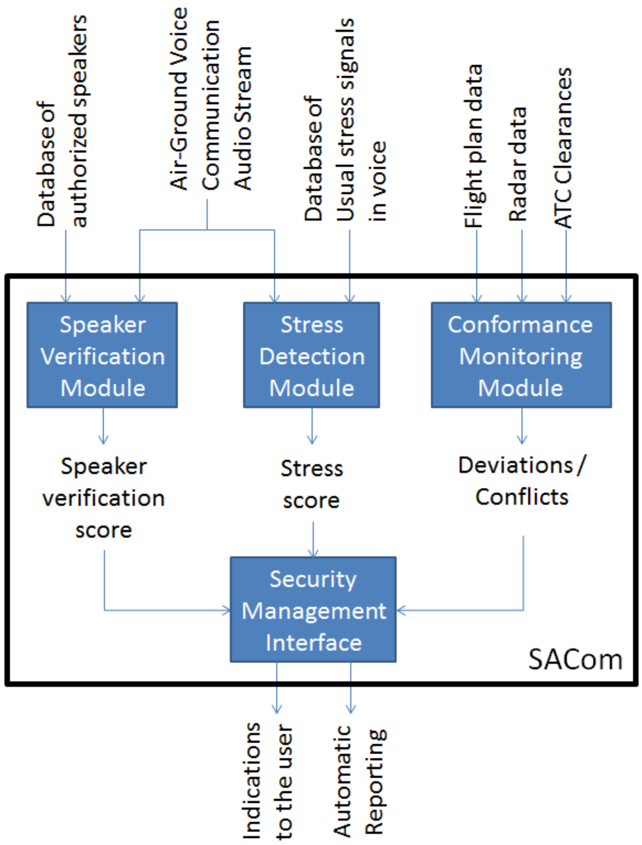
Database of authorized speakers
Air-Ground Voice Communication Audio Stream
Database of Usual stress signals in voice
Flight plan data
Radar data
ATC Clearances
Speaker Verification Module
Stress Detection Module
Conformance Monitoring Module
Speaker verification score
Stress score
Deviations / Conflicts
Security Management Interface
SACom
Indications to the user
Automatic Reporting

FIGURE 1. SACom architecture

Having established the architecture, the system under consideration can be built finally. The consecutive step then is the establishment of appropriate validations. This needs to be done in order to show the feasibility of the new prototype and its usability, usefulness and the trust it is inspiring to people interacting with it. Looking at the SACom prototype the overall vision is to improve the security of the VHF voice communication in ATC. The prerequisite to set up meaningful validations is now the definition of validation objectives.

For SACom the main validation objectives turned out to be [11]:

- Improving the detection of unauthorized participants to the VHF voice communication system
- Improving situational awareness of ATC controllers as well as pilots
- Acceptable performance regarding false alarms, correct detection, usefulness and trust

When the validation objectives are determined the next decision needs to be taken about the suitable validation activity, facility / environment and experiment design.

4. HITL SECURITY SIMULATION CHALLENGES

4.1. General Validation Requirements

Any validation activity can involve different methods mainly covered by model based simulations or real-time simulation. Expert's judgement, paper based validations or shadow-mode trials shall not be withheld. However, what they have in common is the goal to investigate the specific impact of a new system, concept or procedure. This is usually done by comparing the situation including the specific development (solution) with a reference situation (baseline). Both, the baseline and the solution should be set up with the same pre-conditions and pre-settings as well as involving the same events at the same time or following the same time schedule.

For validating security issues in real-time simulations this is not possible because of the nature of a security incident. Usually, such a security incident appears without any pre-warning. It may harm a part of the system or a process where it is considered as very unlikely. This means it is neither expected nor is there any backup or contingency procedure prepared. In addition, security incidents can be sophisticated intentional actions, which means they are complex and it is likely that standard countermeasures (as it may be done in case of safety incidents) do not mitigate the impact. As soon as humans play an essential role, the reaction to security incidents rather requires a high level of awareness, flexibility and improvisation to be successful.

As a consequence, when using human in the loop simulations it is not recommended to compare a baseline with an identical solution scenario which was conducted by the same participant as human in the loop. The reason for this is that the human operator would be much better prepared and pre-warned in the identical second run, making his reaction unrealistic.

Further requirements of validation in general are the need for a good comparability between different validation runs and a high level of repeatability.

In the following, several general aspects are described that were found when preparing and planning the validation activities within the GAMMA project. These points can serve as a guideline for other security validation activities using human in the loop simulations.

4.2. Avoidance of raised attention

To create a realistic encounter of the human operator with the security incident it is important that he or she is not briefed about the upcoming event or the purpose of the simulations. Otherwise, just by the knowledge that “something” will be happening in the simulation, the level of attention of the test person is higher than it would be in the real environment, which distorts the results.

Also a good balance between the number of events and the time periods where normal operations are simulated is of significant importance. These periods of normal operations can nevertheless be designed as demanding, because this way the human operator likely falls back into his or her working routines.

Training sessions, which are performed to prepare the test person to the exercises, shall be designed to impart knowledge and awareness about the framework conditions, the modelled environment and the simulated processes of normal operations without causing any precognition that there will be an (security) incident.

4.3. Avoidance of habituation effects

Especially for complex and memorable events like security breaches a test person develops a special attention and thinks about possible countermeasures and reactions in the aftermath. When he or she encounters the same or a similar event a second time within a few hours or days, these thoughts are still in mind and can directly influence the reaction, also distorting the results.

This is in fact a real problem when validating security issues with the traditional baseline-solution comparison. Ideally, for the purpose of validating security, the test person shall experience exactly the same event only once; i.e. all simulated events shall be as different as possible.

4.4. Maintaining surprise effects

The success and impact of a security attack often depends on the surprise effect. In a real environment, this effect can very roughly be described as the lack of preparation, training, knowledge, procedures, experience or awareness about an incident happening. This effect can be reduced for likely events by an appropriate training and prepared contingency plans/procedures, but not for unforseeable incidents.

In order to maintain this surprise effect, the preparation and briefing of the test person in terms of security shall be kept to a minimum in the frame of the simulation campaign. In addition to that, the simulated security events shall be as smart, unforseeable and unique as possible.

4.5. Modelling of security incidents

A security attack may be very complex and especially in air traffic it may be a highly dynamic process. Similar to safety related incidents (accidents), a lot of different ingredients must work together in the right order with the right timing to cause a specific effect or impact. If any of these factors is different the effect or impact can also be significantly different. As a consequence, all conceivable aspects which may play a role for the replication of the incident must be accurately defined in a simulation. This is also to achieve comparability between consecutive runs with different test persons working on the same scenario. Additionally, all effects of the attack should be reproduced with a high level of detail to be able to investigate all imaginable consequences.

As security incidents usually have an intentional nature, it is to be expected that the attacker will try to sidestep or counteract to applied countermeasures. If possible in any way this should also be simulated.

4.6. Modelling of options

Depending on the purpose of the simulation and the actions expected from the participant, the options available in reality shall be reproduced to a certain degree. Unfortunately, for security issues it is very likely that there is no defined procedure, making it difficult to select appropriate options to react. It is also possible that the participant wants to perform actions which originally stem from other contingency procedures. Anyway, due to the complexity and unpredictability of security events it is expected that the test person will use best judgement to solve the problems with a high level of creativity and flexibility. For this purpose, the simulation must offer several options to (counter)act, which are (almost) equal to corresponding possibilities in real life.

However, the training and briefing should inform the participant about all actions that can be taken in the simulation without giving any hints about upcoming events.

4.7. Sensitivity of data

When setting up HITL simulations another important aspect touching legal issues and data protection issues needs to be considered. Having humans participating to simulations implies the possibility to record data which might be abused regarding e.g. sensitive personal data or performance capabilities of participants. Therefore measures need to be put in place, which secure especially this kind of data and protect it from unauthorized access.

In order to achieve the secure handling of sensitive personal data it is recommended to adhere to well established regulations. Application of and alignment to the list below has proven to reach a sufficient degree of protection and to ensure the integrity and security of data during a project:

- Article 8 of the European Charter of Fundamental Rights (protection of personal data) [12].
- The Treaty on the Functioning of the European Union [13].
- A strategy and methodology based on the Data Protection Directive [14].

When participants for a study are recruited, some necessary personal information relevant to the study (e.g. experience of work, age, gender) will be stored electronically in computers on a hard drive. This data needs to be protected and must therefore not be stored in cloud solutions, portable hard drives or USB sticks. This data needs to be password protected and only accessible to authorized persons.

During such a study only necessary data has to be acquired and stored electronically. This data also needs to be strictly anonymized or pseudonymized, password protected and only accessible to authorized persons. Participants furthermore are allocated a unique number instead of their first- or surname. This number shall be assigned randomly at the beginning of a study. Such a procedure ensures that it will not be possible to somehow associate the data to individual persons. Thus, the data cannot be used to judge or assess the professional capabilities of the recruited participants or how they act in critical situations. Taking these measures into account the recorded data is purely a means to investigate general cognitive processes without risk of leaking personal sensitive information.

5. APPROACH

Taking the framework conditions from above into account there is still the need to set up a realistic environment where the simulated scenarios will be installed and the validation exercises take place. The choice of the simulation facility obviously has a remarkable effect on the success of validations.

5.1.1. Simulation Facility

The Air Traffic Management and Operations Simulator (ATMOS) is an experimental facility for simulating air traffic in real time. In a simulated airspace, the ATMOS can be used to test e.g. new procedures, ATM concepts or supporting systems in terms of safety, feasibility, efficiency and traffic capacity. This facility allows researchers and air traffic controllers to jointly evaluate new working methods for controlling and influencing air traffic.

The simulator is primarily designed for performing assessments with interacting participants, which is why the traffic situations have to be simulated in real time. The assessments relate to technical air navigation services issues from the perspective of air traffic controllers. It is generally possible to use any airspace in the world, including one or more airports as desired. If necessary, the selected airport can be adjusted in line with different air traffic control sectors.

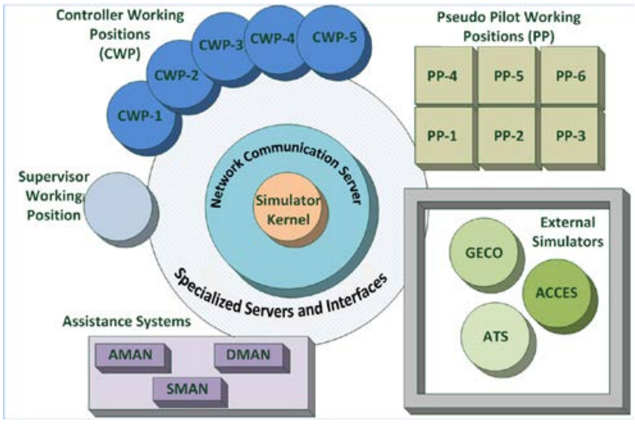
Controller Working Positions (CWP)
CWP-1
CWP-2
CWP-3
CWP-4
CWP-5
Pseudo Pilot Working Positions (PP)
PP-4
PP-5
PP-6
PP-1
PP-2
PP-3
Supervisor Working Position
Network Communication Server
Simulator Kernel
Specialized Servers and Interfaces
External Simulators
GECO
ACCES
ATS
Assistance Systems
AMAN
DMAN
SMAN

FIGURE 2. Simulation facility ATMOS

As shown in FIGURE 2 the ATMOS facility consists of five Controller Working Positions (CWP), a Supervisor Working Position and six Pseudo Pilot working positions (PP). The Air Traffic Generator used to establish simulated traffic is the NARSIM (NLR's Air Traffic Control Research Simulator). The system is completed with a flexible software solution (YADA) for Voice over IP (VoIP) communication between controllers and pseudo pilots.

This simulation facility was selected to be the validation platform to conduct the security validation of the SACom prototype.

5.1.2. Overall Validation Process

One of the main aims of the project discussed here was the translation of SESAR guidance material into general validation procedures for security prototypes and concepts. Following the approach of GAMMA a holistic security management was postulated [15]. The continuous process of (i) inventing the concept, (ii) developing and enhancing it, (iii) unveiling the strategy and planning of validations, (iv) and (v) setting up of different types of validations and (vi) refeeding the results in order to achieve an evolution of the concept was experienced as straightforward (FIGURE 3) and elaborated in more detail hereafter.

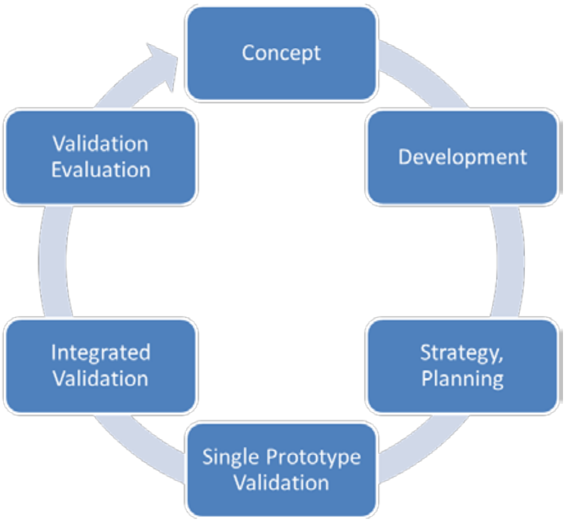

FIGURE 3. Validation process approach

5.1.3. Realization of simulation scenarios

In this section, a short overview of the applied experimental design for the SACom validation exercises is given. This design was identified to satisfy validation objectives, validation requirements and the challenges identified for security validation. The SACom validation exercises were conducted in October 2016 in Braunschweig using DLR's radar simulator ATMOS. Six Air Traffic Controllers participated in this campaign.

One complete exercise consisted of the following steps:

1) Briefing:

The test person was provided with background information about the simulated environment and the specific task to be performed.

2) Speaker Verification Enrollment and Enrollment Verification:

   This short session was necessary to customize the system under validation to the test person.

3) ATMOS Training:

   A short simulation was conducted to familiarize the test person with the simulator, the HMI and with the airspace. This run was already used to collect data as reference for the stress detection module (baseline).

4) Short simulations block:

   A set of 20 short simulations (3-6 minutes per simulation) was performed where the SACom system was running in the background but without indications. In this session the baseline situation (the performance of the controller without any support) as well as the best-case solution (the performance of the system) were directly compared in terms of speaker verification, conformance monitoring and conflict detection. In these short scenarios different events were simulated which directly led to a deviation (non-conformance) of a single aircraft from the given ATC clearance.

5) SACom Briefing

   Now the test person was briefed about the SACom system, its purpose and its abilities.

6) SACom Training

   Another short simulation run was performed to give the test person the chance to get familiar with the security prototype system.

7) One long simulation containing a complete attack

   In this simulation a complete security incident as described by GAMMA was performed. In detail this means there was a simulation phase in which an “unauthorized” person tries to insert fake ATC clearances with the goal to cause a loss of separation or at least some confusion and delay. In this simulation, the test person was supported by the new SACom system. This was mainly done to get qualitative feedback from the test person (expert’s judgement).

8) Debriefing and Questionnaires

   In this part of the validation exercise, several standard and tailor-made questionnaires regarding system usability, situational awareness and trust were applied.

All validation steps, settings of the simulator, of the equipment, the data to be collected and the simulation scenarios are described in detail in a so called storyline document, which also served as a handbook for the very complex experimental design (compared to other validation activities).

5.1.4. Consideration of mentioned challenges

This section describes how the challenges identified in section 4 were considered in the design of the simulation trials conducted in the frame of the GAMMA project. This shall give an example on one hand; on the other hand it can serve as inspiration for similar experiments in the field of security validation.

5.1.4.1. General Validation Requirements

In order to avoid conducting the same simulation scenarios twice (as “baseline” without and as “solution” with the SACom system in place), it was decided to compare the performance of the unsupported human operator (=”baseline”) with the pure technical performance of the system. This was done in exercise step 4 (short simulations block). The SACom was running in the background without any indications to the user (hence operator). It was assumed that the technical performance of the SACom represents the best case situation, provided that the information it produces is immediately realized and correctly considered by the user. The advantage of this approach is that both (assessing the performance of the unsupported human and the pure system) can be covered in parallel in the same simulation run while the frame conditions and traffic constellations are exactly the same for both aspects.

Another option would have been to conduct the baseline and the solution with two different participants. The advantage here would be that there is the possibility to compare both, baseline and solution simulations as it is usually done in validation. The disadvantage is, that two persons are needed per exercise which should have nearly the same experience, level of routine, way of working and competence. In the likely case this is not assured to 100% the results can be distorted again.

Repeatability and comparability between different exercises was achieved by setting the boundary conditions of all simulations in a very stringent way. All short-time scenarios (of exercise step 4) contain a pre-defined traffic situation while every simulation run only took 3-6 minutes, which radically reduces the variability of the traffic flow. This allows provoking specific events with a high level of reliability for every exercise.

The long simulation run (in exercise step 7) contained minutely detailed periods of normal operations and an attack phase. During the attack phase the frequency of actions of the attacker was also restricted: the person simulating the attack was instructed to perform one action at least every 3 min, but not more than every 90 seconds.

5.1.4.2. Avoidance of Raised Attention

Exercise steps 1) Briefing and 3) ATMOS Training were exclusively focused on the simulation environment, the airspace and the equipment installed at the CWP. Only very little background information about the GAMMA project and no information about the design and functions of the SACom prototype was provided in these steps. The purpose of exercise step 2) was (vaguely) stated as necessary for speech analysis functions.

In exercise step 4) Short Simulations Block, just a hint was given that the pseudo pilots are trained and conduct the simulation according to a storyline document. This was necessary because otherwise simulated security events could easily have been misinterpreted as mistakes of the pseudo pilots or as simulator outages.

More detailed information about ATM security and the applied solutions was given just in exercise steps 5) SACom Briefing and 6) SACom Training. At these steps all necessary data to analyze the baseline situation was already completely recorded.

If there was a chance that a person who already accomplished the exercise run meets a person who is planned for another one, both persons should be isolated against each other or at least instructed not to talk about the trials.

5.1.4.3. Avoidance of Habituation Effects

In exercise step 4) Short simulations block, each of the 20 short scenarios was unique, so that the same event, traffic situation and impact did not appear a second time in the same exercise with the same participant. In order to achieve comparability between different test persons all events contained in these short scenarios were predefined to a great level of detail.

In exercise step 7) Long simulation, the attacker was instructed to act spontaneously with defined time constraints regarding the intervention. According to the situation the goal was to cause a critical loss of separation or at least a significant delay. Therefore, also all actions of the attacker were unique and unforeseeable.

5.1.4.4. Maintaining Surprise Effects

As already mentioned, no security specific information was given to the participants in exercise step 1) and 3). In addition to the uniqueness of the different scenarios and simulated events they have been designed to be of unexpected nature. As an example, one short scenario contained a sudden climb of an aircraft which was already established on the final segment of the instrument landing system (ILS) approach. As an ILS provides vertical guidance it is very unusual that an airplane starts to climb without reporting a go-around to the controller. Therefore this manoeuver was absolutely unexpected and was not noticed by the majority of controllers who took part in the mentioned validation campaign. The background of this manoeuver was an intentionally inserted false ATC instruction by an unauthorized person to discontinue the approach and to start the climb.

5.1.4.5. Modelling of Security Incidents

During the simulations, the features and effects of the attack were reproduced as far as possible.

Separate communication channels were installed in the simulator to enable the pilots to hear the voices of the controller as well as of the attacker. In turn, the controller was only able to hear the voices of the pilots but not the voice of the attacker. This should simulate kind of terrain shading which is a normal effect for radio communication. Nevertheless, both channels could leed to a so called “block-out” at the pseudo pilot station similar to radio interference effects in the real world.

The pseudo pilots were trained especially for these simulations to imitate the confusion and a realistic reaction to the events. Airplanes which just entered the sector were simulated in a way that they do not have any information about the things just happened as it would be in real life, even if they are also handled by the same pseudo pilots. In addition, a complete storyline document was written with specific steps and instructions to the pseudo pilot for every single scenario. This storyline contained also instructions how to react in case of foreseeable actions of the controller.

5.1.4.6. Modelling of Options

The simulation setup offered several options to the controller, which were comprehensively explained in exercise step 1) Briefing and 3) ATMOS Training. These options represented several realistic actions in an ATC center. In detail, these simulated options were:

- To give holding instructions to airplanes
- To report to the ATC watch supervisor, which was simulated by an exercise observer
- To coordinate with neighbor sectors
- To accept no more approaches
- To ask for technical support

Unfortunately, a simulated backup frequency could not be installed in the simulator. However this was explicitly briefed to the participant.

5.1.5. Data protection – the legal constraint

Another important prerequisite for the conduction of validation exercises when taking the legal viewpoint is the availability of the described data protection measures for sensitive personal data. Therefore also the issues raised in section 4.7 were taken into account and a procedure to meet the requirements of data protection was invented. Nevertheless, a couple of sensitive data needed to be recorded in order to evaluate the validations.

The prototype under consideration focuses on speaker verification and detection of mental pressure of air traffic controllers and pilots while working. For this purpose speech data was recorded during the validation experiments amongst others. All over the following data elements which were stored:

- Personal profession data.
- Speech / voice data.
- Simulated radar data.
- Observations / questionnaires.
- Administrative data.

The above data was secured by means of data security and the following actions were taken:

- All recorded data was pseudonymized.
- Agreement of all involved persons was acquired (i.e. a declaration of consent needed to be signed).
- Speech / voice and simulated radar data will not be published directly. Only derived data e.g. detected stress, error rates of speaker verification, may be published anonymously.

- All administrative data will be strictly separated from any personal data recorded during validation experiments.
- The simulation facility was locked and access is provided only to authorized personnel.
- During experiments at least one of the authorized persons was present and supervised all activities in the room.
- All computers were located within the simulation room, were password protected and connected to a separate firewall protected LAN.

5.1.6. Psychological aspects

As one last remark, the participants were exposed to several security incidents in one exercise run. These incidents could lead to a simulated loss of separation or even a collision between two simulated aircraft. In reality this would mean a significant safety risk or a loss of lives, which could cause a psychological strain. Therefore it is important to remember the participant of the experimental nature of the simulation and that these kinds of experiments are very valuable to close down security gaps before any incident happens in real life.

6. CONCLUSION

The aim of this paper is to describe the challenges to validate ATM security prototypes and the measures needed to overcome the lack of methods and means for such an application. The aim is also to show how validation of ATM security prototypes and concepts can be set up and conducted. Within the presented work this was implemented by combining and adapting well-known methodologies like SecRAM and E-OCVM. This approach is discussed and enhanced by a detailed description of the activities taken to set up a realistic environment, to achieve impartiality of the test persons and to receive meaningful results.

The described approach can be used as a guideline to validate security prototypes developed for application in air traffic management. The approach is exemplified describing the needed prerequisites and procedures for validation of a dedicated prototype. The stumbling blocks which appeared when designing ATM security prototype validation exercises are listed and discussed for this prototype.

The content of this paper is applicable to security related HITL simulations. Looking at the successful validation results from GAMMA it can be stated that the approach to combine E-OCVM and SecRAM is promising. The developed new kind of simulations has proven to successfully evaluate usefulness, usability and trustworthiness of security prototypes within simulated environment while impinged with security threats. This, however, is true for HITL simulations, where humans are part of the system to be validated.

7. REFERENCES

[1] Roxbee Cox, H. Looking Forward: Prolegomena for a Detailed Study of the Future of British Civil Aviation, 1940, the Journal of the Royal Aeronautical Society, 44(357), 681-754. doi:10.1017/S036839310010255X.

[2] Aeronautics and Space Report of the President, 1971 Activities, Executive Office of the President National Aeronautics and Space Council Washington, D.C. 20502.

[3] EUROCONTROL: European Operational Concept Validation Method, E-OCVM v3., 2010.

[4] FAA, Eurocontrol: Operational Concept Validation Strategy Document, OCVSD v2.0a, 31 March 2008

[5] International Civil Aviation Organization (ICAO): Safety Management, Annex 19 to the Convention on International Civil Aviation, 1st Edition, July 2013

[6] SESAR (Single European Sky ATM Research) Programme, http://www.sesarju.eu/

[7] NextGen (Next Generation Air Transport System), https://www.faa.gov/nextgen/.

[8] Asgari, H., T. H. Stelkens-Kobsch, P. Montefusco, L. Abhaya, R. Koelle, G. Markarian, G. D’Auria, 2017, Provisioning for a Distributed ATM Security Management: the GAMMA Approach, IEEE Aerospace and Electronic Systems Magazine, in press.

[9] SESAR Joint Undertaking, "SESAR ATM Security Risk Assessment Methodology," - Project 16.02.03 D02, 2013.

[10] GAMMA consortium, 2015, D2.1 - Threat analysis & evaluation report.

[11] Stelkens-Kobsch, T. H., A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke and C. Neeteson, "Towards a more secure ATC voice communications system," 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, 2015, pp. 4C1-1-4C1-9. doi: 10.1109/DASC.2015.7311419

[12] Charter of Fundamental Rights of the European Union, Official Journal of the European Union (30.3.2010) No. C 83/389 – 403.

[13] Consolidated Version of the Treaty on the Functioning of the European Union, Official Journal of the European Union (30.3.2010) No. 83/55, article 16.

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities (23.11.95) No. L 281/31 – 39.

[15] GAMMA Consortium, GAMMA Concept of Operations, 2015, http://www.gamma-project.eu/.