From Preparation to Evaluation of Integrated ATM-Security-Prototype Validations

Meilin Schaper, Tim H. Stelkens-Kobsch, Nils Carstengerdes
Institute of Flight Guidance
German Aerospace Center (DLR)
Braunschweig, Germany
Meilin.Schaper@dlr.de, Tim.Stelkens-Kobsch@dlr.de, Nils.Carstengerdes@dlr.de

***Abstract*— It is quite easy to set up validation trials and measure the benefits of one prototype by using well-established validation techniques. But things are getting worse if more than one new system is involved in the evaluation and to make it even more complicated the systems are geo-distributed over different partners' sites. How to cope with the amount of possible combinations of several security prototypes developed in a European aviation security research project? And how to prepare, setup and perform the needed geo-distributed validation trials? These questions will be answered in the paper also detailing a specific validation exercise to describe the approach chosen. The paper will finish with lessons learnt and the outlook to further research topics.**

Keywords—ATM; security; validation; prototype

I. INTRODUCTION

Security in aviation has been a concern since the beginning of commercial aviation (e.g. the hijacking of a Pan American mail plane in 1930 by Peruvian revolutionaries, the explosion of a United Airlines flight in 1933 over Chesterton, Indiana due to a bomb) [1][2]. Awareness was increased in the early 1960s, when the number of hijackings increased [3]. Since then the world experienced not only the absolutely inconceivable terroristic attacks of 9/11 but many others (cf. [1]). These incidents triggered the community of states, institutions and companies to put more emphasis on reducing the vulnerability of air traffic management to the lowest achievable level. The succeeding process led to Annex 17 of the Convention on International Civil Aviation (first adopted 1974) [4][5][6]. Recent attempts of aviation security seem to aim at the more visible part of security (e.g. limitations on gels and liquids for air travelers). However, security in the air traffic domain is still an underdeveloped topic in some specific areas when a more detailed view is taken. Many authors criticize that the aviation domain is mainly responding after security threats occurred instead of proactively working on protecting against the next security threat [1][4]. Reference [4] describes a recurrent pattern in aviation security, which consists of attacks, more stringent security measures as a result of this attack, a following decrease of recurrence, a relaxation phase and new shock phase caused by the next attack.

But why is this passivity regarding security threats so common and widespread in the aviation domain? One reason might be the heterogeneous landscape of systems which are used in air traffic management, which opens up hundreds of possible entry points for exploitations. It is obvious that perfect security is achieved when all vulnerabilities and weak points of a system are secured. This, indeed, is a pious hope as security breaches will never be eliminated completely and in reality the idea of security is interwoven with other Key Performance Areas existing in the ATM environment (e.g. safety). To face the challenges of a secure system which is still flexible enough to serve the wide community of stakeholders it is indispensable to imagine a holistic concept, which takes all user needs and stakeholders' requirements into account.

Following the argumentation above a consortium of industry and research institutions transferred the idea of a holistic and proactive security system in the air traffic management to a project proposal and was elected to conduct the planned work under the project name GAMMA (Global ATM Security Management).

II. BACKGROUND

The GAMMA project is proposing a new operational concept to address security issues in the new global ATM scenario defined within SESAR [7]. Thereby, GAMMA is complementing and extending the scope of SESAR security activities to ensure a comprehensive assessment of the full set of security threats and vulnerabilities affecting ATM and minimizing the effects of ATM crisis brought about by security incidents. The Operational Concept of GAMMA [8] includes roles and procedures for the day-to-day operation of ATM security and the management of crisis at European level. The concept describes a network-centric management framework that needs the support of technological solutions (prototypes) to facilitate the detection of security incidents and exchange of security information between stakeholders (cf. Fig. 1). Although GAMMA provides mitigation measures, the main focus lies on a fast and reliable detection of threats. Implementing the developed security prototypes into the ATM system will improve the situation awareness, result in faster detection of security threats and, in turn, offer more opportunities to mitigate those situations. The latter is true due to more options for actions and/or earlier start of

The research leading to the results presented in this paper has received funding from the European Union FP7 under grant agreement n° 312382. More information can be found under http://www.gamma-project.eu/.

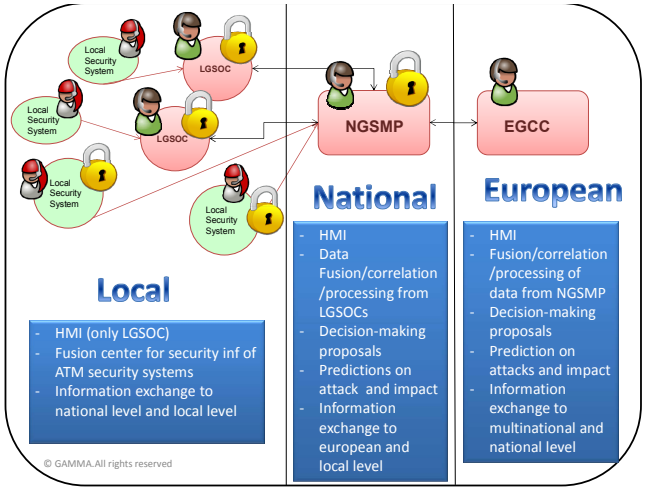

Fig. 1 Overall GAMMA solution [9]

countermeasures. Even ATM actors not under attack can be informed in order to increase their awareness concerning possible coordinated attacks. Ultimately this may prevent future attacks.

As the GAMMA vision is to adopt a holistic approach for assessing and delivering solutions for ATM security, the global objective defined for GAMMA is to demonstrate the improvement in security management in case of security incidents. However, considering ATM as a system of systems environment, it is not feasible to entirely investigate all threats and impacts. Thus limitations to the validation of this holistic approach must be set. These limitations stem mainly from the developed prototypes with its different conceptual horizons and maturity levels (V1 to V3 in accordance with the proven Concept Lifecycle Model advocated by the European Operational Concept Validation Methodology [10]). To accommodate with this, the validation activities consisted of several steps and followed an ATM-security-incidents-centered approach instead of a purely prototype-driven approach. The list of possible threats, worked out in the concept phase of GAMMA [11], was examined to select a subset which is covered by the seven GAMMA security prototypes: P1-P6 (serving mainly as event detector) and the 'Security Management Platform' (SMP), analyzing data from the other prototypes and disseminating information to different security layers (cf. Fig. 2).

In the first iteration, seven comprehensive single prototype validation exercises have already proven the feasibility, the functional and operational capability of the individual GAMMA prototypes using the selected threats [12][13][14].

For the second iteration, combinations of different threats are performed during the validation exercises, attacking a national or the European ATM system. By using the Security Management Platform and its connected security prototypes, the usefulness of the GAMMA concept is shown to GAMMA operators and GAMMA users on a higher level than in iteration 1. Combinations of two threats each are chosen for each validation exercise (see Fig. 3). These threats should be detected by two different prototypes and managed by a national or the European level of SMP. The partially integrated exercises distinguish additionally between uncoordinated and coordinated attacks on national level. The culmination of the validation activities is the full GAMMA Solution, analyzing security incident management at the European level. To achieve this, a European level SMP is integrated with two national level SMPs. Each national level SMP in turn is integrated with two other prototypes. This setup is stimulated with one attack to both nations simultaneously and an additional uncoordinated attack concerning one nation. The objective of this exercise is to show the capability of the newly developed approach to differentiate between different kinds of attacks, draw valid conclusions and suggest appropriate countermeasures (including proper dissemination to military and civil authorities on national and European level).

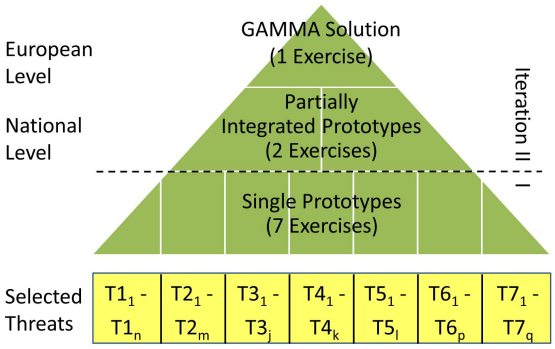

Fig. 2. Validation activities overview

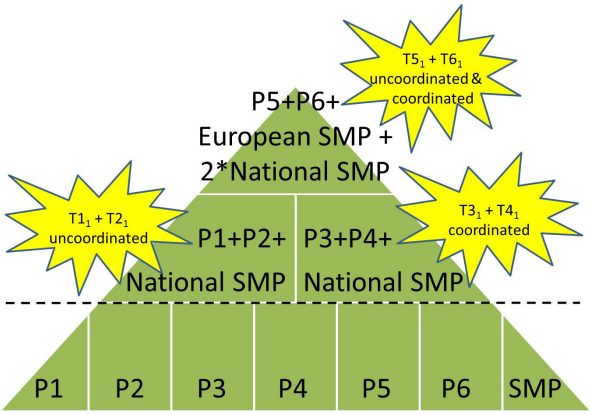

Fig. 3. Selected threates and prototypes for second validation iteration.

Obviously, the performed validation exercises only represent a sub-set of the ATM system. Nevertheless, considering all validation exercises, the whole is more than the sum of its parts and a higher level and more complete ATM environment is evaluated and benefits will be shown.

On the basis of the second validation exercise of the iteration 2, the procedure and challenges of preparing, conducting and analyzing a geo-distributed human-in-the-loop real-time simulation of security attacks will be described in the following chapters.

III. Partially Integrated Exercise 2

The partially integrated exercise 2 (PI2) belongs to the second iteration in Fig. 2 and Fig. 3 and dealt – in addition to general GAMMA concept feedback – with specific questions concerning the detection of coordinated attacks and incident management on national level [15].

Within the validation scenario the test persons were faced with two pre-selected threats: a false ATCo introducing commands into the air-ground voice communication of an approach center and a denial of service attack to AEROMACS (Aeronautical Mobile Airport Communication System) used as airport surface data link. The matching security prototypes to deal with these threats are 'Secure ATC Communication' (SACom) [16] to detect the false ATCo and the non-conformance of aircraft to the real ATCo instructions, 'Information Security System' (ISS) to detect and enable mitigation of the denial of service attack to AEROMACS, and 'Security Management Platform' (SMP) to collect, fuse and visualize security related information on national level. Thereby, operators of the SMP are able to discover formerly unknown correlations between security incidents happening in different locations within one country, draw conclusions, disseminate this information and suggest mitigation and solution strategies. This is expected to lead to quicker reaction times and an increased awareness regarding security attacks.

Three partners of the GAMMA consortium were involved in preparation and execution of the PI2 validation exercise: The German Aerospace Center (DLR) as exercise leader and being responsible for the SACom prototype, Leonardo company (Italy) being responsible for ISS and SMP prototypes as well as providing test persons for SMP and ROMATSA (Romanian Air Traffic Services Administration) providing ATCos as validation exercise participants.

A. Storyline

It was assumed that SACom was installed at the approach center for a mid-sized airport with one of two runways in use. Voice radio was used to communicate between aircraft and approach. Aircraft communication with the tower of this airport was done via an established datalink connection using AEROMACS, which was incorporated in the ISS prototype. The go-around procedure of the airport crosses a STAR which is in higher altitude. The place, the false ATCo used his radio equipment was well chosen: his radio transmissions were received by the aircraft but not by any ground station [16].

The steps of the coordinated attack were the following:

1. Wait for following situation: One aircraft will use the above mentioned STAR, another aircraft is on final and a departure is already on the runway and ready for takeoff.
2. Make a denial of service attack to AEROMACS, so that the departure did not get the takeoff clearance in time. It will stay on the runway.
3. This will trigger the aircraft on final to perform a go-around and follow the standard go-around procedure.
4. The false ATCo intrudes the frequency and instructed the aircraft going-around to climb to an altitude that conflict with the aircraft on the STAR.

The ISS prototype was expected to detect the denial of service attack and send an alarm to national SMP. Using SMP the GAMMA operator shall notice the alarm and select pre-defined countermeasures which will be sent to and applied by ISS. The SACom prototype shall detect an unauthorized speaker i.e., the false ATCo and send this alarm to SMP. Additionally, if the aircraft going-around starts deviating from the standard go-around altitude, a conformance-monitoring alert shall be sent to SMP. SMP is expected to detect that those alarms are caused from a coordinated attack and display this to the GAMMA operator. The GAMMA operator is expected to notice the alert, and to use SMP to select and send countermeasures in time.

B. Setup

The validation exercise was set-up as a geo-distributed human-in-the-loop real-time simulation (cf. Fig. 4). SACom and its validation environment were located in Braunschweig, Germany, the other two in Italy: ISS in Florence and SMP in Chieti. Web-conferences were used to share the screens in all locations. Braunschweig served as exercise lead and supervision, so additionally to the local SMP event viewer the screen of the SMP test person acting as GAMMA operator and the ISS screen were displayed in a web-conference.

The storyline was implemented as an extensively tested and fine-tuned traffic scenario enhanced with matching temporal instructions for the persons conducting the attacks to ensure a realistic, coordinated and harmonized flow of events for the test persons.

C. Participants

Nearly twenty persons were needed to perform the PI2 validation exercise. Two participants were invited to take part in the exercise as test persons, five more to support as independent experts. The other participants acted as technical staff, validation lead and validation support at the three different locations.

ISS required no test person; all necessary actions were done by the simulation team. As SACom was not subject of validation itself, it needed no test person. But, as the security incidents had to be a surprise for the participating ATCo, four ATCos from ROMATSA were invited. Those ATCos were not involved in any exercise preparation.

SMP required a test person acting as GAMMA operator. Two Leonardo company employees did this task in Chieti. To widen the scope of impressions, one human factors (HF) expert of DLR acted additionally as GAMMA operator in Braunschweig during the execution of the final test run. Here the SMP was

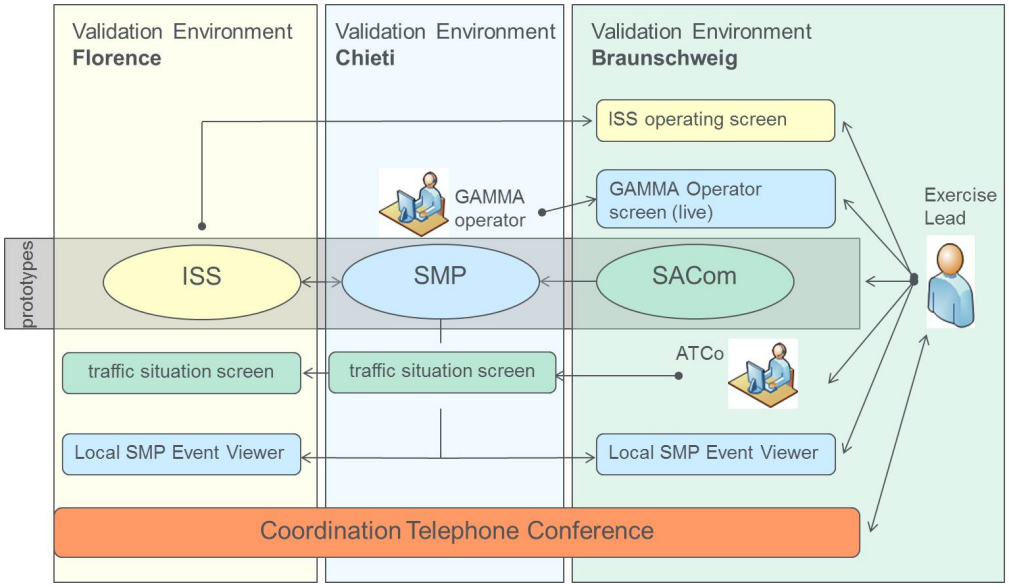

Fig. 4. Schematic representation of the geo-distributed validation setup; arrows indicate the data flow.

operated using the local SMP event viewer, which served the same output- and input modalities as the SMP used in Chieti with one difference: there was no connection back from the local SMP event viewer to SMP. Actions like selecting countermeasure were possible – but without effect.

The participants taking part in this validation exercise as operator were asked to give their feedback regarding the feasibility and usefulness of the GAMMA concept, ATM security in general and also about prototype functionalities, usability and the simulation setup. Therefor both bespoke and well-established, standardized validation questionnaires were prepared by human factors experts together with operational experts and engineers of the involved prototypes. These extensive and thoroughly reviewed set of questions was given to the participants as one online questionnaire with different subsections. For each statement in the questionnaire five possible ratings are available to the participants, indicating strong disagreement (1) to strong agreement (5) to the according statement.

D. Execution

During two days in May 2017 four exercise runs were performed, cf. Table 1.

Table 1: OVERVIEW EXERCISE RUNS

	Run	**SMP operator**	**ATCo**	**Exercise Observer**
	Final_test	HF expert	Internal	
Day 1	PI2_1	SMP_op#1	ATCo#1	
	PI2_2	SMP_op#1	ATCo#2	ATCo#1
Day 2	PI2_3	SMP_op#2	ATCo#3	
	PI2_4	SMP_op#2	ATCo#4	ATCo#3

1) Location Florence

As ISS required no test person and the simulation team was aware of their tasks, no specific briefing or debriefing was necessary.

2) Location Chieti

Before the exercise started, the SMP test persons, one at a time, were briefed about the GAMMA concept, the SMP concept and how to operate the SMP. A trained observer assisted the test person during the exercise in case of questions. One test person supported the first day the other one the second day, simulating a SMP operator working shift each. It was of no concern to use the SMP test persons for more than one run, as their job is specified to handle security incidents in normal operations

Both test persons were de-briefed and answered the questionnaire after the exercise runs.

3) Location Braunschweig

Before the exercise started, the ATCos were briefed about the airspace (including procedures) and trained how to use the working position. They entered speech utterance into the system; these were used by SACom's speaker verification module to calculate their personal identification [17][18]. But, by intent, the involved prototypes, their functionalities and the storyline of the following exercise runs were neither mentioned nor visible to keep the ATCos unaware of the following security attacks. The task of the ATCOs was to handle the

traffic and work normally. To induce variance within the validation scenarios for the SMP operator, each ATCo performed only one run.

During the exercise a trained observer assisted the ATCo in case of questions and noted all remarks of the participant. These remarks were also used to guide the following debriefing. The debriefing was additionally used to explain the participant's work as part of the whole, giving information about SACom and its functions, the PI2 exercise, including ISS and SMP functionality, and the GAMMA concept in general.

4) Joined Exercise

Participants briefing and debriefing was done locally, whereas the exercise conduction was done jointly. A telephone conference was used for coordination of the following events: Start of the exercise, coordination of the attack, end of exercise and technical/organizational debriefing. Fig. 5 shows the exercise lead working position in Braunschweig, which was additionally used to control the SACom validation environment.

After completing their exercise run, two of the ATCos took the opportunity to observe the next run mainly focusing on the security concept implementation. A human factors expert supported the ATCo during the observation. Valuable feedback gathered during the observation and debriefing was used to complement the results of the SMP test persons.

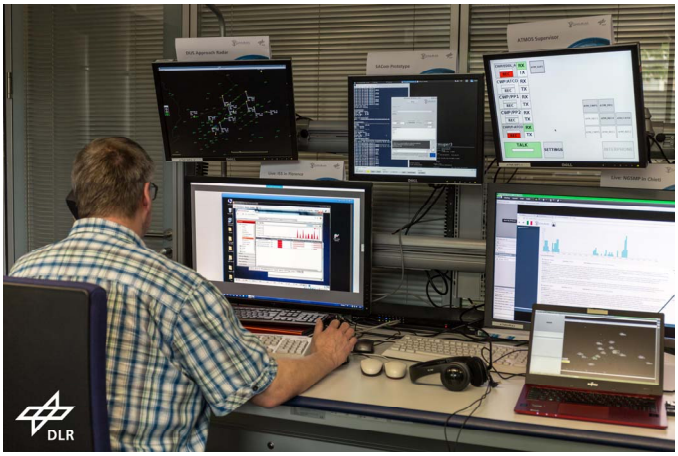

Fig. 5. Exercise lead working position showing from upper left to lower right: approach radar screen, SACom speaker verification module, simulation control interface, ISS interface, SMP viewer, web-conference-screen.

E. Results

Summarizing the main results of the questionnaire and the debriefing sessions, a general agreement to the approach taken with the GAMMA concept could be shown. The results are depicted in Fig. 6 and Fig. 7. More specific, the combination of information about security attacks on national level was rated as useful, supporting the operators in post-event analysis of security events and enhancing the ATM security in general. Strong agreement could be observed regarding the benefit of disseminating security-relevant information as described by the concept. The security information reaching the national level are mainly the right ones and derived recommendations on national level provided a benefit compared to recommendations at local level. However, areas of improvement have been identified regarding the trust in recommended countermeasures and its presentation.

Analyzing the results in Fig. 7, which are dealing with the incident management on national level, a generally positive trend can be observed. The participants were able to detect a joint attack by using the national SMP. Despite a high variance in the data, there was a slight agreement that the national SMP supported in detecting security attacks in general and correlated attacks in particular. Recommendations about countermeasures were by trend seen as useful and as a support for decision making, helping in selecting countermeasures. Despite the general agreement that the information provided by national SMP can improve the incident management on national level the participants were not sure if they would like to have the information provided by national SMP in their daily work. This may be due to the fact that the national SMP displayed a lot of information regarding the attacks, used a high degree of textual information (instead of graphic visualizations) and did not filter/aggregate updates of already received information. Besides, the role of the SMP operator does not exist in the ATM world nowadays. The participants found it hard to imagine themselves to work with the new security management platform (in addition to their normal work tasks), however, the general benefit of such a system was acknowledged.

IV. Conclusions

The idea of the GAMA project is to provide a proactive approach to enhance security in the air traffic domain. By using a new, holistic operational concept to address security threats, different security prototypes have been developed and validated. First validation exercises dealt with single prototypes on a local level. But as the project proceeded, more complex threat scenarios were evaluated. These threat scenarios considered the holistic claim of the concept by involving different attack locations on national or European level and different coordinated and uncoordinated attacks happening at the same time. One example of such a complex, geo-distributed security validation activity with three security prototypes was described in this paper.

The conclusions are structured in three sections: First, the results of the validation exercise itself and the implications concerning the underlying security concept. Second, lessons learned regarding the planning and execution of complex, geo-distributed validation activities involving different prototypes. Third, the next steps in evolving the conceptual approach to a holistic, European aviation security management will be described.

It may be recalled that the goal of the validation exercise described in this paper was to provide evidence that the security approach taken in the project is meaningful and delivers benefits compared to the situation today. The results

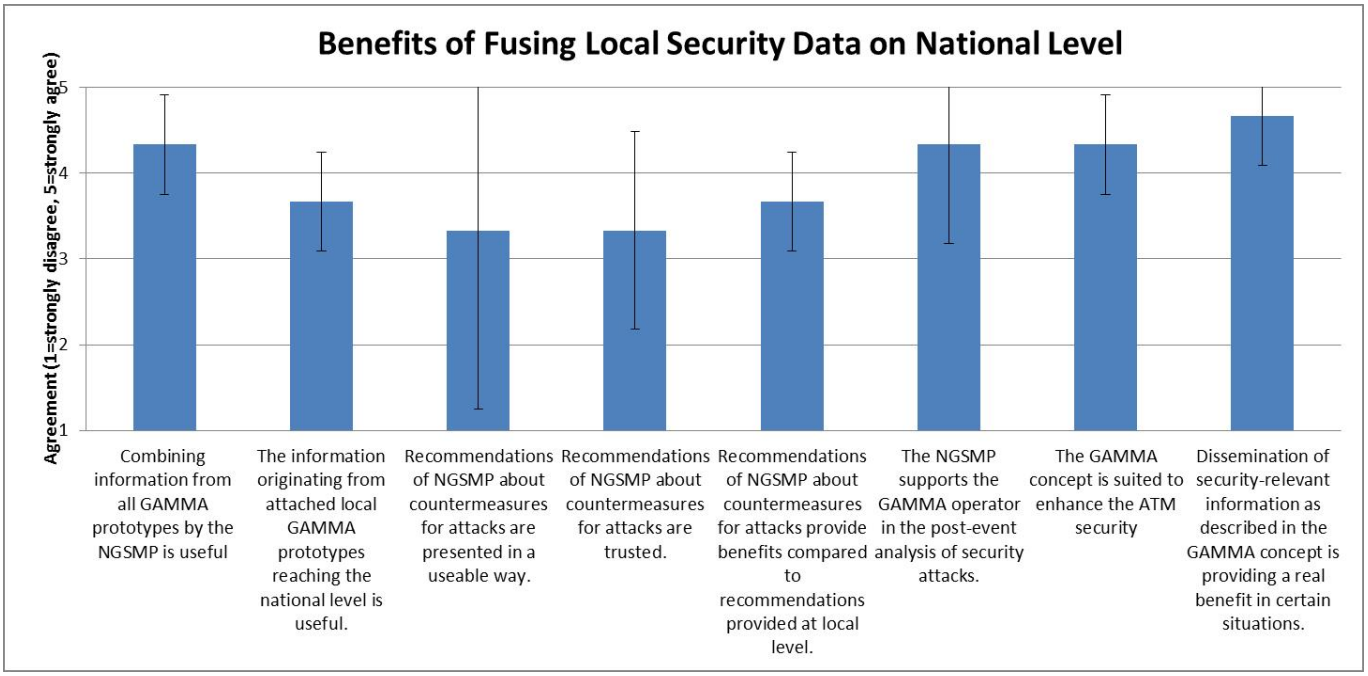

Fig. 6. Benefits of fusing local security data on national level

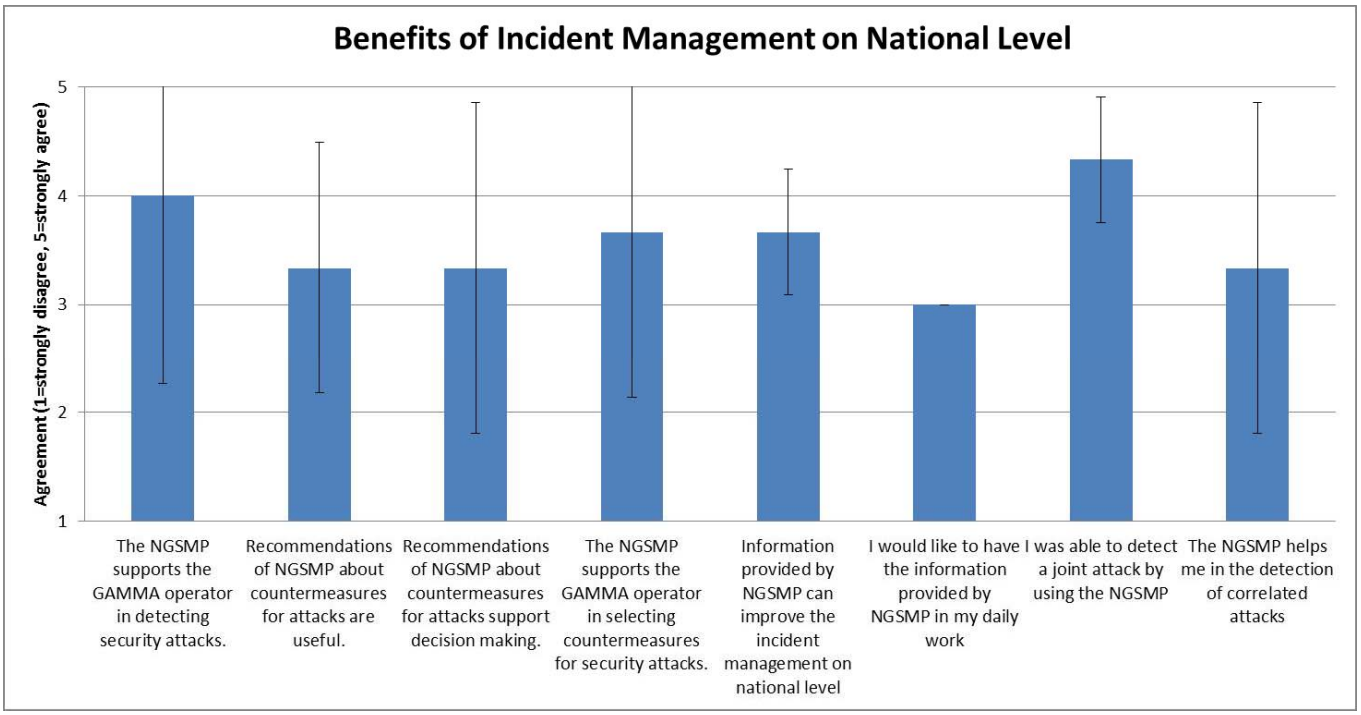

Fig. 7. Benefits of incident management on national level

of the validation exercise indicate general agreement to this assumption. Especially, this holds true for certain aspects of the new security approach: Combining information about attacks on a higher level (such as the national level) were highly appreciated. This information can serve multiple purposes like post-event analysis, dissemination of security- and threat-related information to interested stakeholders (and maybe next targets of attacks) and the general enhancement of ATM security management by providing timely information. Benefits were seen in the detection of attacks and the new possibilities to correlate attacks to discover formerly unknown connections. This information offers the opportunity to support

decision making and to suggest recommendations about appropriate countermeasures. Challenges for the future have been identified with regard to the presentation of such complex information and the connected issues of situation awareness, trust and usability of the technical systems.

For the first time, a geo-distributed validation environment with locations all over Europe was used to simulate multiple security threats happening in one nation. Tremendous efforts were needed to achieve the goals set before. A viable approach, which was applied successfully in this project, is to write a validation plan in early project phases to develop a mutual understanding of definitions, concepts and the way forward. Partners had very different areas of expertise but one common goal: improving security. The discussions leading to the validation plan were needed to understand and align the different expectations e.g. using fast-time simulations or highly sophisticated human-in-the-loop real-time simulations with a clear focus on concept validation. This correlated with the question if, when and how to involve external experts as test persons. An additional and connected discussion developed about which data need to be recorded, its frequency, and how to process and analyze them including data protection issues in different countries. Accompanying to the project development, ideas and prototypes evolve and may change compared to the initial conception. Therefore, it is vital to the project success to have regular discussions and to keep the initial plans updated. This fosters consensus on the chosen approach. During the preparation and execution of the exercise it is important to train the locally responsible persons of all participating sites to act as a team in the geo-distributed situation and to follow the same strict rules and procedures in conducting the exercise, brief and debrief participants, start and stop of runs to guarantee the necessary quality of the results.

The results of the security concept validation exercises are promising. Some results have been reported in this paper and in [12]. However, some refinements are needed to improve benefits of the proposed approach. In order to tackle security threats in a holistic, proactive manner there is the urgent need to better interlink civil and military authorities and decision-makers conceptually and operationally. Considering the impact single – or even worse multiple, coordinated – security attacks can have on the European air traffic management, communication and collaboration on European level is vital. Therefore, the conceptual approach takes these aspects (European security management layer, civil-military coordination) into account. Nevertheless, these aspects need a thorough review and validation, involving subject matter experts of all concerned stakeholders.

Taking the results of the already conducted exercises into account, three topics for further work can be derived:

1) The security prototypes under test proved their fitness for purpose. Yet areas for improvement could be identified in the design of the human-machine interfaces and in the way information and alarms are interchanged and disseminated.

2) Although the GAMMA concept already defined roles and responsibilities on national and European level, there is still the need for specifications and legal confirmation of these procedures. Furthermore, the local level has to be taken into account by clarifying new responsibilities and new mitigation means in case of attacks and the impact of new procedures on liability issues.

3) The security concept described in this paper identifies two new roles in the management of ATM security events: the SMP operator on national level and the one on European level. To really live up to expectations put into these core roles in the security concept, more work is needed regarding essential and required skills (e.g. experience in the ATM domain to interpret security alarms and their impact correctly). Selection procedures and training needs of candidate SMP operators may also serve as material for further research.

The advocated concept of this paper follows a proactive, layer-based and network-centric approach of a security management platform with different and flexible security prototypes serving as event detectors. We think that this is a promising approach to enhance aviation security and worth to be explored further.

ACKNOWLEDGMENT

The authors would like to thank our project partners Leonardo company and ROMATSA, as well as the DLR simulation support team, for supporting and participating in the validation.

REFERENCES

[1] M.F Schiavo, “A Chronology of Attacks against Civil Aviation” in Aviation security management, Andrew R. Thomas (Ed.), Praeger Security International Westport, Connecticut,. 2008., pp. 142-260.

[2] U.S. Attorneys´ Bulletin Vol 52 No 01, Transportation and Terrorism – usab5201; 2004; https://www.justice.gov/sites/default/files/usao/legacy/2006/02/14/usab5201.pdf

[3] G. Elphinstone, “The Early History of Aviation Security Practice”. in Aviation security management, Andrew R. Thomas (Ed.),. Praeger Security International Westport, Connecticut, 2008, pp. 1-8

[4] M. Karimbocus, “The Human Element” in Aviation security management, Andrew R. Thomas (Ed.), Praeger Security International Westport, Connecticut,. 2008., pp. 50-64

[5] M.A. Alemán, “The International Civil Aviation Security Program Established by ICAO” in Aviation security management, Andrew R. Thomas (Ed.), Praeger Security International Westport, Connecticut,. 2008., pp. 65-76

[6] ICAO Annex 17 to the Security Convention on International Civil Aviation, 10th edition, 2017

[7] http://www.sesarju.eu/

[8] GAMMA Consortium, “GAMMA CONOPS”, Rev. 01.00, 2015 http://www.gamma-project.eu/docs-publications/.

[9] GAMMA Consortium, D4.1 – ATM Security Requirements, 2015, unpublished

[10] European Organization for the Safety of Air Navigation (EUROCONTROL) “European Operational Concept Validation Methodology (E-OCVM)”, Volume I, Version 3.0, February 2010.

[11] GAMMA consortium, D2.1 – Threat analysis & evaluation report, 2015, unpublished.

[12] T. H. Stelkens-Kobsch, M. Finke, M. Kleinert, M. Schaper, „Validating an ATM security prototype – first results“, Digital Avionics Systems Conference (DASC), 2016

[13] GAMMA Consortium, D9.1 – Release 1 Validation Report, 2017, in press

[14] Tim H. Stelkens-Kobsch, M. Finke, N. Carstengerdes, "A Comprehensive Approach for Validation of Air Traffic Management Security Prototypes", Digital Avionics Systems Conference (DASC), 2017 – in press

[15] GAMMA Consortium, D5.1 – Validation Exercise Plan , 2015, unpublished

[16] 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, 2015.

[17] A. Ridzik; M. Rusko,."PLDA Speaker Verification with Limited Speech Data". in International Conference on Speech and Computer,. Springer, Cham, 2015, p. 325-332.

[18] M. Rusko; M. Finke, „Using speech analysis in voice communication: A new approach to improve air traffic management security" in: Cognitive Infocommunications (CogInfoCom), 2016, pp. 000181-000186.