Addressing Security in the ATM Environment

From identification to validation of security countermeasures with introduction of new Security Capabilities in the ATM System context.

Patrizia Montefusco
Traffic Control System Engineering
LEONARDO
Naples, Italy
patrizia.montefusco@leonardocompany.com

Rainer Koelle
School of Computing and Communications
Lancaster University
Lancaster, United Kindom
rainer.koelle@eurocontrol.int

Rosana Casar
Department of Transport and Information Technology
ISDEFE
Madrid, Spain
racasar@isdefe.es

Tim H. Stelkens-Kobsch
Institute of Flight Guidance
German Aerospace Center (DLR)
Braunschweig, Germany
tim.stelkens-kobsch@dlr.de

***Abstract*—**

This paper addresses the full lifecycle of security countermeasures identified in the Security Risk Analysis of the future Air Traffic Management System (ATM). The process establishes new security functions identified in the GAMMA project [1] and their implementations in order to ensure acceptable levels of security for ATM.

In this project, ATM Security is addressed by focusing on two dimensions defined by Single European Sky ATM Research [2]: establishing a collaborative support capability by defining a framework embracing three-levels for Security Management (i.e. European, National, and Local) and developing security measures for the self-protection/resilience of the ATM Systems by exploiting automated security-related functions to handle potential threats.

This paper concentrates on the second dimension and how the countermeasures are identified, implemented and developed in prototypes. The prototypes will then be validated in an operational scenario, through the new concept introduced by the project.

The reader will be accompanied through a practical example of the whole process on how ATM Security needs have been identified. The objective is to protect the core ATM Security functionalities (Primary Assets) and corresponding Supporting Assets. We identified 44 of the most feared threat scenarios in terms of impact on the SESAR Key Performance Areas (KPA). The threat scenario described in this paper is "False ATCO", affecting the Supporting Asset "Voice system". The developed prototype is "SACom" (Secure ATC Communication) that considers the security countermeasures identified in the risk treatment analysis to reduce the risks. The paper concludes with the description of the activities planned for validating the SACom prototype as part of the proposed global solution.

Key words: ATM Security, Validation, Self-Protection, Cyber-Security, Security Management

I. INTRODUCTION

Recent events impacting Air Traffic Management (ATM) Security not only have unveiled the existing security vulnerabilities and capability gaps, but the urgent need to efficiently and consistently respond to attacks; and if possible to anticipate future attacks. It is commonly known that attackers are in a continuous learning process, looking for exploiting vulnerabilities and countermeasures that are put in place for protecting the assets. The fact that security measures are predominantly devised and deployed after vulnerabilities have been exploited has contributed to the perception that security is mostly being addressed in a reactive manner.

ATM Security is not a fundamentally new problem. Initial work on ATM Security started in the aftermath of the 2001 September 11th attacks and major critical infrastructure incidents in 2003. Since then new concepts and requirements have been introduced such as the establishment of an organisational Security Management System within Air Navigation Service Providers (ANSP) as stated in the European Implementing Regulation IR1035/2011[3] .

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

One of the main on-going activities related to ATM Security is being led by SESAR but political priorities shaped the work on ATM Security during the SESAR Development Phase. Its current approach focusses on the establishment of security requirements and objectives as part of the system engineering process. The actual implementation of associated security solutions is left for the Deployment Phase. In order to support SESAR, the new concept or approach addressed in this paper postulates the establishment of an ATM security function as an additional service of the air navigation system. This service provides dynamic security management and incident management capability, including collaborative support.

The remainder of this paper is structured as follows. After the brief introduction in Section I, Section II shows the proposed approach for the management of security in the ATM system and introduces the new security function. Section III defines the security solution concept. Section IV analyses the emerging risks in the ATM environment and defines new Security Key Performance Indicators (KPI). Section V elaborates ATM security requirements and the architecture of the proposed concept by taking into account the countermeasures previously identified. Section VI describes how the proposed Security solution will be validated. Section VII concludes the paper and discusses the plan for further work.

II. CONTEXT ESTABLISHMENT

This lack of a built-in security capability was the main driver behind the Global ATM Security Management project (GAMMA). Funded under the 7th Framework Programme of the European Union, the project aims at building a holistic solution for ATM Security. The project approaches security management in a comprehensive manner. The activities flow from an extensive security risk assessment, enabling the definition of requirements and architecture components for a set of security capabilities in the future air navigation system, through the demonstration of the interplay and modes of operations of the devised capabilities through a set of validation exercises. The demonstrators form a part of the aforementioned functions and sub-systems that may be embedded in the ATM/CNS system context. In that respect, some of the demonstrators developed during the project lifetime reflect security enriched prototypes for ATM/CNS system components (i.e. supporting assets from a security risk assessment perspective).

A. Security Function Approach

Today, ICAO Annex 17 and Doc 9985 both recognize the role of air navigation service providers and stakeholders within the wider field of aviation security. ATM Security is now defined in two dimensions:

1. self-protection and resilience of the air navigation system; and Security Function
2. collaborative support to other aviation system stakeholders.

This definition allows for a first conceptualization of an ATM Security Function. The primary purpose of air navigation is to ensure the safe, orderly, and efficient flow of air traffic. Accordingly, a security function needs to ensure the security of the associated air navigation systems and services to the airspace users and all participating stakeholders. From a self-protection/resilience perspective, the dynamic management of security across the air navigation system requires a security management capability that is an embedded function within the air navigation system (c.f. Fig. 1 below).

Such a security function is intended as the operational, procedural, and technical means to realize a desired air navigation system capability. Understanding the set of security solutions as a function allows for a clear separation from sub-systems or system components while establishing a clear interface within the air navigation system context and relevant security actors.

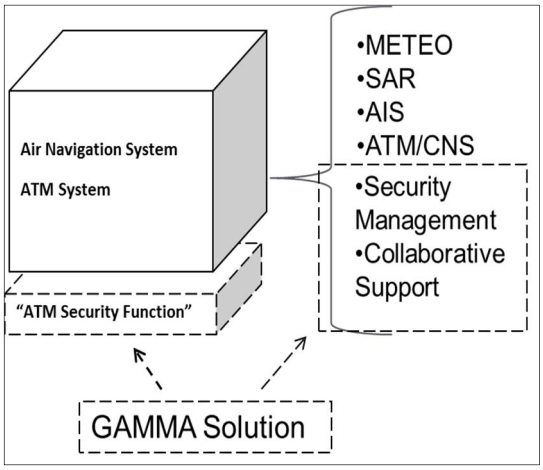

Figure 1 The new ATM Security function

B. Solution Conceptual Overview

From the security function, a holistic security solution is proposed. It revolves around the integration of security solutions within the ATM System to establish a system-wide holistic Security Function. It has been driven by a state-of-the-art (defined by the regulatory framework and the existing ATM Security solutions) and by a rigorous security risk assessment (adopted from SESAR) considering the challenges of the highly interconnected ATM System. These drivers informed the development of a concept of operations, that supports the deployment and required security operations within the ATM system. The solution comprises a combination of organisational and technical controls to manage the security of the ATM System and range from preventive controls to incident management support. These controls are conceptualised as a network of distributed nodes collectively supporting the dynamic management of security. In order to address the dual nature of ATM Security, this solution comprises the following elements [3]:

- Organisation – two types of roles are distinguished: Operators and ATM stakeholders who jointly collaborate in the management of security. The Operators play the manager role in terms of the security situational awareness and they operate the systems specifically designed for this solution. On the other side, the users are the classical ATM stakeholders who will be the beneficiaries of the information generated by the proposed security solution.
- Situation management/incident management capability – the set of functions and capabilities (including associated operational procedures) to manage the security of the ATM System and security incidents.
- Distributed network and information exchange – the technical communication means for the day-to-day management (i.e. situation and incident management).

In summary, the Organisation includes the human aspects of the solution and the other two elements are represented by a set of security (sub-) system interconnected to different levels of scope (local, national and European). The latter will be represented by the prototypes to be developed in order to validate the solution.

C. *Solution Supporting Assets and Prototypes*

In order to support the development of this solution, a high-level operational architecture is defined. It comprises the set of supporting assets of the ATM/CNS context including the devised security capabilities (i.e. prototypes) developed by GAMMA [17]. This architecture is depicted in the figure below.

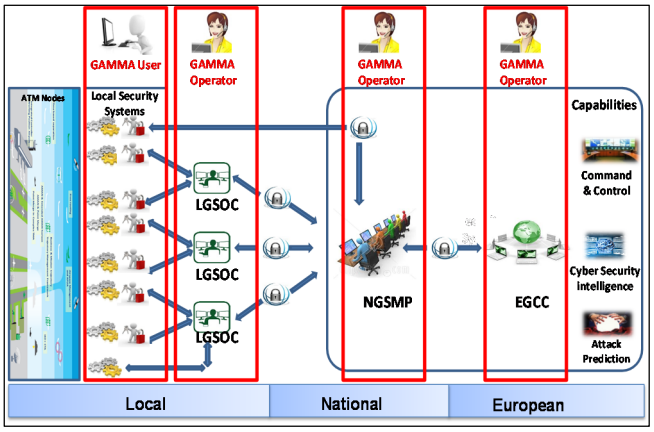

Figure 2 the proposed GAMMA solution

On one hand, there are two types of human actors who can be differentiated by how they use the solution. The operators represent the subset of actors that directly interface with the specific security solution components. They perform the regular and continuous security management activities and - in particular – the security incident/situation management operations.

On the other hand, the users include all relevant stakeholders interconnected to the proposed solution through their dedicated systems or interfaces. They will be provided with relevant information concerning the ATM system state, its service assurance, and further information related to their profile articulated in form of the 'need-to-know' principle. This allows for the integration of non-classical ATM Security stakeholders like national aviation crisis cells, governmental authorities, etc.

The main goal of this physical and logical infrastructure is the demonstration of a proposed security concept through a set of validation exercises. In order to address the concept of operations, following solutions are conceived for:

- security management capability by developing a national security management platform, including a supporting information dissemination system and threat prediction functions;
- security services in support of ATM/CNS components, in particular
    - Network-level: information exchange gateway and information security system.
    - Communication: RF jamming detector, SATCOM security, integrated modular radio, GNSS communication, and secure ATC communication.

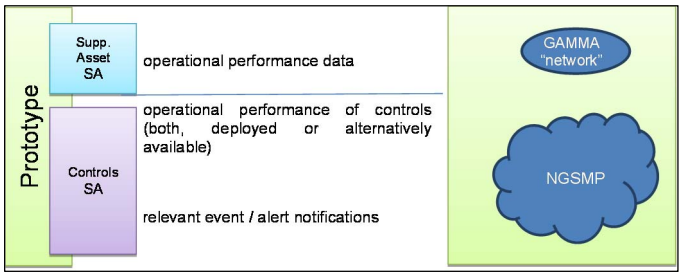

Figure 3 – GAMMA Principal Information Relationship

Regarding the systems supporting the solution three different levels can be distinguished depending on their geographical scope:

- *Local security system and Local GAMMA Security Operations Centre (LGSOC):* The local security systems represent the technical security controls typically deployed on a local level embedded into the supporting asset and may be enhanced by organisational and operational controls. These systems may be directly connected to the network (either to local or to national level) or managed locally (e.g. logical access control). A local security operations centre (LGSOC) is managed by an operator. It represents the principal fusion centre for monitoring the local security situation regarding the status of the

supporting assets under local control (e.g. CNS infrastructure/service) and the respective security controls (e.g. secure ATC voice communication [4]). A LGSOC ensures local access to non-local capabilities (e.g. network intrusion detection, threat prediction) and situation/incident management related information exchanges dependent on the role of the local centre (e.g. security alerting).

- *National GAMMA Security Management Platform (NGSMP):* This component is the national reporting centre for a set of local security systems and/or LGSOCs belonging to the corresponding nation. It is also operated by an operator. This level is provided with additional control capabilities for the continuous dynamic security management which are not available on the local level or complement the local level functions. Furthermore advanced and intelligent functions are in place to support the security situation management operations.
- *European GAMMA Coordination Centre (EGCC):* The EGCC is identified as a pan-European coordination centre of ATM related security information managed. Previous research has identified the lack of a consistent cross-border coordination capability across Europe. To complement the national coordination, the EGCC is designed to relay relevant information on security across different States beyond the national/adjacent state space, and to ensure timely coordination with international parties (e.g. other ICAO regions), regional/global organisations (e.g. European Network and Information Security Agency), and incident management functions (e.g. European Aviation Crisis Coordination Cell).

This solution is going to be validated (partially) through different demonstrators. They are structured in two categories here: the ones related to the local security systems and other ones related to NGSMP and EGCC level.

In our example, the relevant prototypes are:

- *Security Management Platform (SMP)* implementing the levels corresponding to the NGSMP and EGCC. Therefore the SMP will be the core component of the proposed technical solution. SMPs will form the working environment/operating centre on national and European level and it will provide the functionality for the management of security throughout all phases, from prevention to identification of security incidents and the efficient resolution of the resulting ATM Security incidents. The main intelligence and coordination within the postulated security system will rely on the SMP.
- *And Secure ATC Communication (SACom)* being part of the local level*:* SACom operates as a local security system. It detects the intrusion into air-ground voice communication by a person giving false instructions to aircraft with the intention to disrupt the safe and efficient flow of air traffic. The functionalities and the interaction of the different modules incorporated in the SACom prototype have been described in [7].

The local security systems cooperate with and are connected to the LGSOC and NGSMP. The prototype described in this paper, SACom, considers the security countermeasures identified in the risk treatment analysis to reduce the risks [7].

III. ANALYSING THE RISKS IN THE ATM ENVIRONMENT.

The scope and boundaries of the discussed concept are defined through the Security Risk Assessment relying on the SESAR SecRAM [8], the ISO 27005 [9] based security risk assessment methodology developed by SESAR that is tailored to be applied to the European ATM context.

In order to ensure consistency and avoid overlapping with the work performed within SESAR from a technical point of view, It has been used a top-down approach for security. This means that a security risk assessment is performed which looks at ATM as a system of systems, whereas security risk assessments undertaken in the SESAR development phase follow a bottom-up approach for so-called operational focus areas that comprise a series of SESAR projects and developments.

Considering the large perimeter of this study (i.e. European ATM system) and the timeframe allocated to the security risk assessment in this project, a prioritisation has been performed limiting the scope to the most relevant primary assets (ATM core functions), their respective supporting assets (tangible means enabling the core functions) and the highest impact attack scenarios.

Consequently different threats have been explored that can affect the ATM system: cyber threats (i.e. spoofing, distributed denial of data, manipulation of data, media eavesdropping) and physical threats (i.e. RPAS hijacking, aircraft hijacking, and physical damage) by considering internal and external ATM threat agents.

Once the impact and probability of the threat scenarios was assessed, the level of security risk was deduced and then treated to reduce the risk to meet the security objectives initially defined for the respective assets.

The security controls were iteratively identified, firstly through the application of Minimum Set of Security Controls (MSSCs) (as per ISO 27002) developed by SESAR [10] and then - in case the level of risk was not reduced enough - through the definition of additional technical, organisational or procedural security controls. The latter come from three sources: newly identified or devised controls or through refinement of the MSSCs.

Finally, a list of Security Key Performance Indicators (KPIs) was defined in order to provide a measurement reference of the efficiency of the identified security controls. This allows for the quantification and evaluation of the

performance of the proposed technical solution as part of the envisaged validation activities.

A. Security KPI

According to the ICAO Manual on Global Performance of the Air Navigation System, key performance areas (KPAs) are "a way of categorizing performance subjects related to high-level ambitions and expectations". ICAO has defined 11 KPAs: safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, and interoperability. In this paper the focus has been set on the Security KPA, although the system performance may be positively impacted by higher robustness and resilience – ultimately – supporting other performance areas as well.

The expected performance of the technical solution can be quantitatively expressed by means of key performance indicators (KPIs). The set of Security KPIs defined are conceived to provide a measurement of the efficiency of the security controls taking into account each threat scenario analysed in the frame of the Security Risk Assessment and Treatment.

These KPI's are part of the assessment criteria of the validation to measure the effectiveness of specified security controls, developed prototypes and the benefit of the defined security elements. Comparing the KPIs against a defined baseline allows for the identification of the project contributions.

For example, the number of threats detected in time supports ATM Stakeholders in terms of situation awareness (e.g. summary statistics) and allows checking and eventually improving the security of the ATM system.

In the example developed in the next chapter, it will be shown how the security KPI are used in the forthcoming validation exercises.

B. Threat scenario example: False ATCO

A threat scenario is defined in SESAR methodology as the chain of events which takes place starting with a threat source and ending with the consequences of an incident. The scenario originates from a threat source and exploits the vulnerabilities of a specific supporting asset for reaching the primary assets and compromising their level of confidentiality, integrity or availability.

In a congested traffic environment, in non-standard situations, or simply when exchanging air-ground messages in plain language, voice communication is still the basic and most important communication method within air traffic control. In this operational scenario, one of the most feared threats is the intrusion of unauthorised messages (threat) into the voice system (supporting asset). The loss of integrity and availability of the ATM information exchange has a high impact on SESAR KPA (safety, capacity, environment, costs, etc) as shown in the following table.

Supporting Asset	*Threat*	*Primary Asset*	*Reviewed Impact*	*Likeli-hood*	*Risk Level*
Voice system	*False ATCO*	*Arrival management, landing procedure*	*5*	*4*	*High*
		Departure management, take-off procedure			
		Conflict management			

Table 1 Example of Risk level Evaluation

In the risk treatment phase the consortium identified, beyond MSSC, a series of needed additional security controls exploring organizational, operational and technical countermeasures.

Security Control ID	Supporting Asset affected	Security Control Description
ASC_TFA_05	Voice System	Air-Ground voice system in order to be protected from False ATCO shall be supported by means to detect voice pattern anomaly
ASC_TFA_06	Voice System	Each ACC/TWR shall operate and control speaker verification.
MSSC_TFA_01	Voice system	Each ACC/TWR shall have procedures in place that specify when and by whom external authorities (e.g. law enforcement, fire department, supervisory authorities) shall be contacted in the event of a false ATCO

Table 2 Extract of Security Controls

The security countermeasures identified have been used as input in order to identify operational, organisational and technical requirements for defining the GAMMA technical solution.

IV. Defining Requirements and Architecture

Following the definition of the security framework, the scope, and the high level concept, the specification of the proposed solution was undertaken. This has been the intermediate step to translate the conceptual work into specifications to support the development of

systems/prototypes and the validation activities. Two outputs were provided: the requirements specification and the architecture of the security management concept. The requirements answered the question "What should be done to protect ATM environment/systems?" and the architecture answered the question "How this should be done?"

The most challenging aspects addressed in these two activities were the holistic approach, which resulted to be really wide, and the different granularity among the requirements, which was deeper for the systems which were going to be used into the validation activities.

Thus the specification process was iteratively carried out organising the requirements by levels of granularity. Further compromise was found to balance the high-level description of the security controls and the need of concreteness of the developers in charge of the design and development of the prototypes. With the goal of supporting the development of the prototypes and the validation activities, taxonomy for the structure of the representation of the requirements was introduced (See Figure 4). This comprised the inclusion of specific fields like the threat phase (detection, reaction, etc.), the success criteria for considering this requirement as successfully validated, the related KPIs which could be used to assess the requirements, and the indication of the suitable prototypes to implement that requirement.

REQ - ATC Voice		
Identifier	REQ - ATC - 9	
Requirement Description	Voice pattern anomaly in air-ground voice communications shall be detected by technical means.	
Phase	Detection	
Type	System	
Validation Method	Simulation / Experts judgment	
Success Criteria	Earlier detection of voice pattern anomaly than with current system.	
REQ Trace		
Source	ASC_TFA_05	
Threat scenarios	T - False ATCO	
Supporting assets	Voice System	
Prototype	Secure ATC Communication (SACom)	
KPI	Sec_KPI_17	Number of detected dangerous/undesired aircraft behavior events in a defined time frame.
	Sec_KPI_21	Number of unauthorized speakers detected in a defined time frame.

Figure 4 Example of ATM Security Requirements

In addition to this, the traceability in the requirements definition was carefully addressed. This was crucial to justify how and why a requirement was defined. This traceability was recorded in several fields for each requirement.

At the same time and in synchronisation with the requirements development, the architecture of the security management concept was modelled using the NAF (NATO Architecture Framework) methodology. The NAF includes both operational and systems architecture views so that the validation activities and the development of the prototypes could be done appropriately. The architecture went deeper in the specification of the different supporting assets of the solution and it went one step forward defining the information flow and the exchanged data between the different elements.

As an additional activity during the establishment of the architecture, the modelling of the threat scenarios has been carried out in the beginning. This was considered to define the solution and it allowed to have a global view about how the threats may constitute nowadays. This is used as a baseline for building the validation scenarios supporting the validation activities.

According to the example of the threat scenario and in line with the method previously detailed, the requirements have different granularity. Therefore, two sets of requirements apply to address this specific scenario:

The first set is specific to the technical solution related to each threat scenario. The requirements are fully linked to the security controls and the threat scenarios coming from the Security Risk Assessment. The Table 3 contains the list of requirements applying to the controls created to address this specific threat scenario including the related KPIs established (c.f. below).

Requirement description	KPI (ID)	Source
REQ - ATC – 1: Formal exchange policies, procedures, and controls shall be in place to protect the voice system through the use of all types of communication facilities.	Sec_KPI_03 Sec_KPI_07 Sec_KPI_17 Sec_KPI_21	MSSC_TFA_01
REQ - ATC – 9: Voice pattern anomaly in air-ground voice communications shall be detected by technical means.	Sec_KPI_17 Sec_KPI_21	ASC_TFA_05
REQ - ATC – 10: Each ACC/TWR shall operate and control speaker verification.	Sec_KPI_17 Sec_KPI_21	ASC_TFA_06

Table 3 Traceability Security Requirements-Security KPI- Security Controls

The main security KPIs are:

- *Sec_KPI_03*: Number of denial of service attacks detected in a defined time frame.
- *Sec_KPI_07:* Number of disrupted data detected in a defined time frame.
- *Sec_KPI_17:* Number of detected dangerous/undesired aircraft behaviour events in a defined time frame
- *Sec_KPI_21:* Number of unauthorized speakers detected in a defined time frame.

The other set of requirements are generally applied to any system. They should be taken into account when implementing any new system in an integrated environment. These requirements complement the ones related to a specific solution (e.g. ATC Voice system). Their assessment will be performed in the partial and fully integrated validation scenarios. Since the list of requirements is extensive, only a subset related to the integration with the national and European level is listed here:

- EGCC *shall* correlate and store sanitised information/events in a repository.

- EGCC *shall* fuse security data received from NGSMPs.
- The proposed technical solution *shall* address the collaborative support by ensuring the provision of incident support related information, including sanitised data/information to support the activities of the security stakeholders.
- Local security systems *shall* send information (alarms, alerts and monitoring data) to the LGSOC/NGSMP.
- NGA *shall* update security policies in order to define how the capabilities (function and information) provided by the technical solution can be used.
- NGSMP *shall* sanitise information before disseminating to EGCC.
- The process to sanitise data/information *shall* consist of:
    - Identification of the restricted data/information: sensitive and confidential data/information.
    - Identification of the stakeholders that can access to that sensitive information/data.

V. VALIDATING THE SECURITY SOLUTION: PROTOTYPES DEVELOPMENT AND VALIDATION AND VERIFICATION (V&V) ACTIVITIES

The general aim has been to validate and demonstrate security related capabilities on the basis of a subset of sub-system capabilities. From that perspective, the prototypes represent supporting assets within the scope of risk assessment.

Validation activities will be carried out following the European Operational Concept Validation Methodology (E-OCVM) [12] currently used within SESAR. The overall validation approach is depicted in Figure 6 which comprises validation exercises that are performed on the level of the prototypes, combined sets of prototypes, and on the integrated project level.

Already during the inception and planning phase, a holistic approach towards security management was chosen. This view is maintained throughout the validation activities. The process selected to assess this holistic approach is a three-step validation strategy (Figure 5) in line with the three levels defined for the proposed concept in the conceptual phase (Local, National and European).

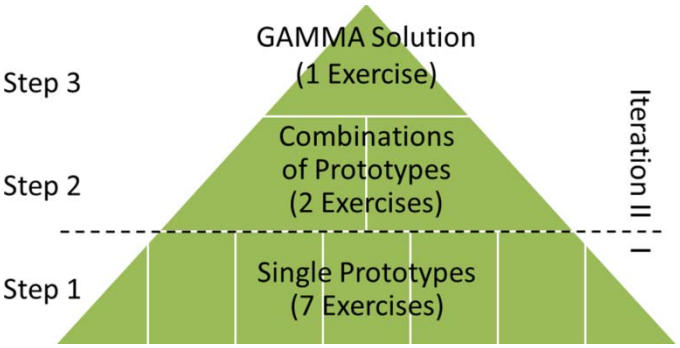

Figure 6 Validation Process Approach

The first stage is focused on the local scope of the concept. In terms of prototypes this is translated in verifying and validating the prototypes and the pre-defined interfaces in isolation (i.e. without connections between different prototypes). The second stage is focused on the national scope of the concept. This reveals the conceptual applicability of the local security systems cooperating and connecting to the NGSMP. A partial integration is foreseen in terms of interconnected prototypes and usage of the dedicated validation environment. To end up, the third stage is focused on the European level and how the overall concept (local security systems-NGSMP–EGCC) can live and work together bringing the expected benefits defined in the concept of the project. In terms of systems and prototypes, this is the most challenging phase in which a full integration between the single prototypes, the subsystems of several prototypes and the validation environment will take place.

As mentioned in the introduction of this chapter, this phase also includes other activities related to systems development such as verification and integration activities. Of high importance for the success of the validation is the integration of this set of heterogeneous systems within a common validation environment. It will be managed through parallel validation/verification activities to ensure a seamless transition between the prototype development and integration phase on the one hand and the execution of the validation exercises on the other hand. Since the emphasis of this paper is placed on the conceptual idea, the further elaboration of the validation activities is out of the scope of this paper.

A. Demonstration on SACom prototype

In order to demonstrate the applicability of the described methodology, the development of one of the prototypes shall now be discussed in more detail. Detailed information about the setup of the prototype is provided in [7].

As the threat “False ATCO” was identified to be one of the most feared attacks on ATM, it was evident to develop this threat with the idea of the proposed methodology. In the previous chapters the risk assessment and treatment was described while here the relevant security requirements for the SACom prototype shall be elaborated. The principle fitness for purpose is shown when a technical means meets the postulated requirements. Consequently the SACom prototype is fit for purpose – and therefore fulfils the research question – if it

satisfies the main requirement to address the threat "False ATCO". As this requirement is somehow blurred it was one of the tasks to split this requirement into more measurable sub-requirements. A subset of the ones found for the threat under consideration are depicted in (Figure 7).

Req. Id.	Description
...	...
REQ - ATC - 9	Voice pattern anomaly in air-ground voice communications shall be detected by technical means
REQ - ATC - 10	Each ACC/TWR shall operate and control speaker verification

Figure 7 Security requirements realized by SACom Prototype

However, the fulfilment of requirements is not the only constraint which has to be met during a validation. Of high importance is also to meet the validation goals which also have to be postulated in advance. The general validation goals found in the project at hand are:

(i) GAMMA-VALG-GEN-1: the ATM environment including GAMMA solution improves security management at local, national and European level compared to the defined baseline situation (without GAMMA solution).

(ii) GAMMA-VALG-GEN-2: the information can be accessed by the proper roles at the right time

(iii) GAMMA-VALG-GEN-3: the sensible information is available only to the authorized roles.

From the above some more detailed (strategy related) validation goals have been derived, which make reference to the different types of validation activities to be performed within the project. For the sake of simplification only the relevant goals for the SACom prototype are listed (Figure 8).

Strategy-related Validation Goal ref.	Description	GAMMA Global Validation Goal ref.
GAMMA-VALG-STR-1	The information about security generated at local level is considered usable by all the roles when a threat is detected.	GAMMA-VALG-GEN-1
...	...	...
GAMMA-VALG-STR-4	The information about security generated at local level is considered beneficial by all the roles when a threat is detected.	GAMMA-VALG-GEN-1
...	...	...
GAMMA-VALG-STR-10	The GAMMA operator can access the information needed to perform its activities (prevention, detection and mitigation).	GAMMA-VALG-GEN-2
...	...	...
GAMMA-VALG-STR-14	Exchanged information and new procedures performed are in line with the current regulations.	GAMMA-VALG-GEN-1 GAMMA-VALG-GEN-2 GAMMA-VALG-GEN-3

Figure 8 Goals for the SACom prototype

For the subsequent work the exercise objectives were defined [18] . These objectives may be understood as a more detailed expression of the general research question and are intended to reach the postulated validation strategy goals (Figure 9). It has to be mentioned that the possibility exists that not every exercise objective can be met in the validations. This results e.g. from constraints resulting from the available validation infrastructure or the achievable level of detail.

Objective ID	*Objective Description*	*Validation Strategy Goal*
Obj.-5_1:	To validate that the detection of a False ATCO is optimized by using the prototype	*GAMMA-VALG-STR-1* *GAMMA-VALG-STR-4* *GAMMA-VALG-STR-10* *GAMMA-VALG-STR-14*
Obj.-5_2:	To validate that the performance of the prototype is acceptable (regarding false alarms, correct detection, usefulness and trust)	*GAMMA-VALG-STR-1* *GAMMA-VALG-STR-4* *GAMMA-VALG-STR-10* *GAMMA-VALG-STR-14*
Obj.-5_3:	To compare the impact of individual prototype subsystems (speaker verification module (SVM), stress detection module (SDM) and conformance monitoring module (CMM)) on threat management	*N/A*
Obj.-5_4:	To validate that the solution leads to a better situational awareness of ATCO regarding appearance of False ATCO	*GAMMA-VALG-STR-1* *GAMMA-VALG-STR-4*

Figure 9 Validation Objectives

After defining the needed assumptions for the forthcoming validation exercises and definition of roles and methods applied in the validations, the system configurations for the baseline and the conceptual solution have been determined.

Within the Validation Plan [18] submitted during the considered project the validation acceptance criteria (VAC) for the fulfilment of the elaborated SACom requirements were found as shown in Figure 10:

VAC-ID	Req-ID	Objective	Acceptance Criteria
...	...	...	...
AC_SACom_6	REQ - ATC - 9	Obj.-5_2	Stress detection module assistance will be accepted by ATCOs
AC_SACom_7	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_8	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_9	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module False ATCOs are detected earlier compared to the baseline
AC_SACom_10	REQ - ATC - 9	Obj.-5_2	With the SACom prototype stress detection module ATCOs situation awareness ratings are improved compared to the baseline
AC_SACom_11	REQ - ATC - 10	Obj.-5_2	Speaker verification module assistance will be accepted by ATCOs
AC_SACom_12	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_13	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_14	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module False ATCOs are detected earlier compared to the baseline
AC_SACom_15	REQ - ATC - 10	Obj.-5_4	With the SACom prototype speaker verification module ATCOs situation awareness ratings are improved compared to the baseline
AC_SACom_16	... REQ - ATC – 9 REQ - ATC – 10	Obj.-5_2	SACom prototype assistance will be accepted by ATCOs
AC_SACom_17	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_18	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_19	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype False ATCOs are detected earlier compared to the baseline
AC_SACom_20	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_4	With the SACom prototype ATCOs situation awareness ratings are improved compared to the baseline

Figure 10 Validation acceptance criteria

The task of the planned validation exercises for the prototype will then be to show the fulfilment of each of the above listed VAC. For the definition of the acceptance criteria

the development of the aforementioned KPI was of high necessity.

B. Partial integration in order to demonstrate the Security Function

The next stage of the validations is planned for spring 2017 and will constitute partial and full integrated exercises. After demonstrating the capabilities of each individual prototype in step 1 and after defining the interoperability between the prototypes and SMP, variable combinations of prototypes will be validated. The partially integrated validation will be based on the interoperability of different prototypes with the national level of a SMP. These steps will analyse the combination and interplay of selected prototypes and the SMP.

The partially integrated validations each utilize some event detector prototypes and a local and/or national SMP. The objective of the partially integrated validations is to validate that the information generated at the local and/or national level is usable/beneficial and reliable for the users and operators of the proposed concept. The promulgation of the local level awareness to the national and European level will be shown based on the Concept of Operations (CONOPS) postulated by the GAMMA project [5].

The partial integration will deliver valuable results and insights to the challenges and obstacles on the way to implement the concept. Up to now there are no results available, although the initial planning for these simulations/experiments is already ongoing.

VI. CONCLUSIONS AND NEXT STEPS

A. Summary

This paper has addressed the whole lifecycle of security countermeasures in ATM. As well the identification as the implementation guided by the proposed concept has been presented. The concept consists of three levels managing the security events according to the geographical scope: local, national and European. The flow of information is specified to be linear (Local to/from National and National to/from European) and also bidirectional if necessary. At this point in time, the conceptual work of the technical solution postulated by GAMMA has been defined [14][15][16][17], as well as the basis for the validation activities, i.e. the validation strategy and the plan for the exercises [18].

The SACom prototype introduced takes into account the security countermeasures defined during the risk treatment phase, to reduce some risks affecting the future ATM System. The SACom validation example has also shown how it is intended to validate that the information generated at local and/or national level is usable, beneficial and reliable for the users and operators. The effectiveness of the security countermeasures is measured within the validation phase with help of the Security KPIs introduced and identified in the project during the evaluation phase.

B. Next Steps

The proposed security management concept expands the toolbox of ATM to achieve a new holistic approach to manage ATM Security. The solution aims at complementing the work already performed within SESAR. Consequently the concept addresses both aspects of ATM Security defined within SESAR, self-protection/resilience and collaborative support, ensuring a seamless approach to ATM Security.

The proposed solution goes beyond the theoretical approach. The validation of the solution will assess the feasibility of the concept through the development of prototypes which will be examined in the validation exercises. The implementation furthermore benefits from automation while providing a complete picture of the ATM Security and the establishment of a reliable collaborative framework. Consequently the security events and threats will be automatically detected and this information will be further processed by the national level. At this level the information will be made available to one operator to support the handling of potential and real threats. In order to establish the collaborative support, sanitised information is sent from National to European level. The opposite flow of information may be established in order to detect and manage security events detached from national boundaries. The project's concept will have to be supported by procedures which should be trusted and agreed among the different parts and involved roles and entities. Thus as part of the collaborative framework tasks, bilateral agreements at different levels will have to be performed. The task of the presented work will be limited to the dissemination activities between the stakeholders and the proposal of recommendations and best practices.

Next steps are the final development and the verification of the prototypes and the validation environment to undertake the validation exercises. The work related to the technical solution will end with the contribution to the security framework in terms of human factors, the introduction of new operational procedures introduced by the proposed solution and regulatory recommendations.

ACKNOWLEDEGMENT

The authors would like to thank all GAMMA consortium members contributing to the development and continual refinement of the concept of operations.

REFERENCES

[1] http://www.gamma-project.eu/

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

[3] (EU) No 1035/2011 "Laying down common requirements for the provision of air navigation services "

[4] International Civil Aviation Organization (ICAO), Doc 9985 AN/492-Restricted, Air Traffic Management Security Manual, Montreal: ICAO, 2012.

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

[6] GAMMA Consortium, D4.1 "ATM Security Requirements", Appendix A GAMMA Concept of Operations Concept, July 2015.

[7] T.H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, C. Neeteson, „Towards a More Secure ATC

Voice Communications System“, Proceedings of DASC 2015, in press.

[8] 16.02.03, SESAR ATM Security Risk Assessment Methodology, D02, 00.01.04, 02/05/2013.

[9] ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management

[10] SESAR ATM 16.02.05-D137 , SESAR Minimum Set of Security Control

[11] GAMMA Consortium, Deliverable D4.1 “ATM Security Requirements”, section 3 Requirements Specification Methodology , July 2015.

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

[13] D. Kolev, R. Koelle, R.A. Casar Rodriguez, and P. Montefusco, “Security Situation Management – Developing a Concept of Operations and Threat Prediction Capability”, Proceedings of DASC 2015, in press.

[14] GAMMA Consortium, Deliverable D2.1 “Validation Exercise Plan”, July 2015.

[15] GAMMA Consortium, Deliverable D2.3 “Validation Exercise Plan”, July 2015

[16] GAMMA Consortium, Deliverable D4.1 “ATM Security Requirements”, July 2015

[17] GAMMA Consortium, Deliverable D4.3 “Validation Exercise Plan”, 2015

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