GAMMA
GLOBAL ATM SECURITY MANAGEMENT

Advances in the provision of Security in ATM

GAMMA project handbook

Advances in the provision of Security in ATM

Contents

Introduction

Advances in the provision of Security in ATM is a handbook, elaborated in the frame of the European project GAMMA, which intends to provide a comprehensive collection of scientific articles on the subject of ATM Security Management, written throughout the 4 year span of the project by the organizations involved in GAMMA.

The GAMMA[1] project stems from the growing need to address new Air Traffic Management (ATM) threats and vulnerabilities due, for instance, to increased reliance on automation and interconnectivity between systems. The goal of GAMMA is to develop solutions to these emerging vulnerabilities backed up by practical proposals for their implementation.

In order to reach this goal, GAMMA first performed a comprehensive assessment of the most feared security threats and vulnerabilities affecting the existing ATM system, considered as a 'system of systems' and covering operational as well as technological aspects. This work was rooted on the new ATM scenarios introduced by the Single European Sky initiative and the Security Risk Assessment methodologies laid down in SESAR[2].

SESAR has represented a constant guidance and reference throughout the work of the project. While not part of the SESAR initiative, the GAMMA consortium made a conscious effort to ensure that the work carried out in the project fitted into the broader context set by SESAR. This is evident in the adoption of the SESAR SECRAM methodology to perform Risk Assessments which resulted in a list of additional Security Controls complementing those already defined in SESAR.

The initial analysis of threats and vulnerabilities provided the basis for GAMMA to develop a new vision, representing a concrete proposal for the day to day operation of air traffic management security. The proposed solution was then tested in exercises using validation platforms encompassing prototypes and demonstrators developed within the project.

GAMMA handbook is divided into 4 sections, reflecting the structure and approach taken by the project in dealing with Security in the ATM domain.

The **first section** sets out the institutional context and includes articles providing a broad vision of the proposed framework within which the technical developments are intended to operate. This section also refers to the Security Risk Assessment which was performed at the start of the project laying down the foundations for all subsequent work.

The **second section** provides the background for the definition of an architecture describing the proposed solution. These articles describe the process through which the broad visions, introduced in the previous section, are translated into detailed architectural descriptions laying the ground for their implementation (described in the following section).

The technical solutions and functionalities are described in **Section 3** of this publication. This section includes articles on the 7 prototypes (and associated modules) developed within GAMMA. These prototypes recreate in an experimental environment the GAMMA concept outlined in section 1 of the book, representing a small scale reproduction of the GAMMA architecture. The prototypes should therefore be seen as a selection from a wider set of security enhancements and functionalities envisaged within the full GAMMA architecture. The Security Management Platform prototype, or SMP, represents the core of the concept, implementing the principles of cooperative management of ATM security outlined in the vision. The SMP is fed by security related

[1] GAMMA "Global ATM security management" is a project funded by the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement nr. 312382. The project started in September 2013 and concluded in November 2017.

[2] SESAR: Single European Sky ATM Research

information sent by the other 6 prototypes, each representing specific security enhancements applied to the ATM domain and providing defence against security attacks at local level.

Finally, **section 4** includes articles relating to the validation activities performed in GAMMA. By integrating the prototypes into a larger validation environment, GAMMA was able to build complex geo-distributed platforms. These platforms provided the basis to implement three integrated validation exercises, demonstrating test cases for evaluating the GAMMA concept with external stakeholders and experts.

The ATM Security solution proposed by GAMMA builds on the principles and concepts related to Security Management in a collaborative multi stakeholder environment, while maintaining a strong link to the current International and European legal frameworks and the constraints imposed by the respect of national sovereignty. The vision of collaborative ATM security management is widely accepted as a principle guiding the implementation of an ATM Security Framework in Europe. GAMMA has contributed to the discussions over the future shape of ATM Security Management by demonstrating how to build on these generally accepted principles, exploring their technological and operational implications and opportunities.

The GAMMA R&D work, spanning from 2013 to 2017, coincided with a period of significant change in the institutional framework defining the management of ATM security in Europe. The initial lack of clarity over the future governance and management of ATM Security was gradually filled with more concrete proposals emerging from the relevant European institutions. While this evolving scenario represented a challenge for the GAMMA project in its initial years, it also opened the opportunity to fill the gap by proposing a vision for the future shape of ATM Security management. Although it is clearly beyond the scope of GAMMA to prescribe specific solutions, as an R&D project GAMMA has endeavored to add an exploratory flavor to the discussions over the future shape of ATM Security Management in Europe.

Worth about fourteen million euros, GAMMA has been co-financed by the European Commission within the Seventh Framework Programme (FP7). The Consortium, led by Leonardo SpA, includes 19 partners representing stakeholders active in the ATM Security domain.

This handbook is presented as a lasting testimony of the work done within the project and as a contribution towards the definition of a Secure ATM system.

***Giuliano d'Auria**, Leonardo SpA*

GAMMA Project Coordinator

Section 1. Security Risk Management and Concept Definition

This section collects papers and articles written by the GAMMA partners concerning the studies developed in the first part of the project: the security risk management of the European ATM system of systems and the definition of the GAMMA CONOPS.

In this project, ATM Security is addressed by focusing on two dimensions defined by the Single European Sky ATM Research (SESAR):

- Developing security measures for the self-protection/resilience of the ATM Systems by exploiting automated security-related functions to handle potential threats
- Establishing a collaborative support capability by defining a framework embracing three-levels for Security Management (i.e. European, National, and Local).

The first paper concentrates on the first dimension and how the countermeasures to protect ATM assets are identified, implemented and developed in the GAMMA prototypes (further described in Section 3). The prototypes are then validated in an operational scenario, through the new concept introduced by the project.

The second paper develops the second dimension of ATM security addressing a collaborative security situation management capability for air navigation. More specifically, the development of a threat prediction capability is treated as a situation management problem by mapping the concepts of situation awareness and information fusion.

The overall purpose of the GAMMA project is therefore to demonstrate a comprehensive approach to ATM security by providing a concrete proposal for the implementation of capabilities to address and manage security risks in a dynamic and collaborative multi-stakeholder contexts. The GAMMA CONOPS describes how the security function is conceptualized through a network of GAMMA operators and users, including local security (sub-)systems or system security functions, representing a network of distributed nodes embedded within the air navigation system. Within this organizational framework and set of technical functions, the GAMMA concept builds a tailored information exchange between the different nodes on three principal levels: Local, National and European.

Civil and Military coordination represents another fundamental aspect of the Collaborative Support dimension. This part of the study, described in the last article of this section, includes aspects related to governance, organisation, procedures, regulations, technologies with the aim of identifying the institutional environment within which the GAMMA proposed solution is intended to operate. This is considered a prerequisite for its smooth adaptation and integration into this environment.

Patrizia Montefusco, *Leonardo SpA*

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)*
***Rainer Koelle**, School of Computing and Communications, Lancaster University (Lancaster, United Kindom)*
***Rosana Casar**, Department of Transport and Information Technology, ISDEFE (Madrid, Spain)*
***Tim H. Stelkens-Kobsch**, Institute of Flight Guidance, German Aerospace Center (DLR) (Braunschweig, Germany)*

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] .

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.

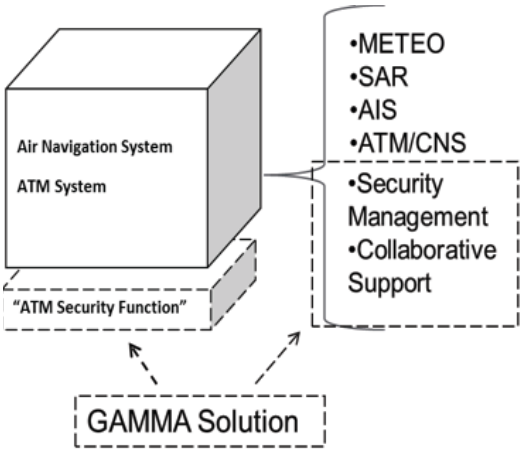


Figure 1: the new ATM Security function

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.

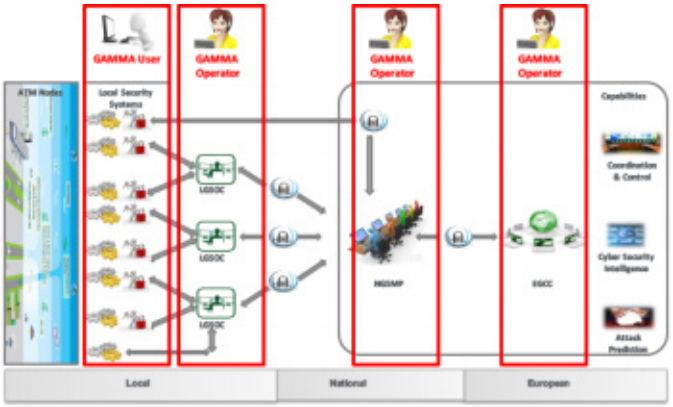


Figure 2: the proposed GAMMA solution

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
  - o Network-level: information exchange gateway and information security system.
  - o Communication: RF jamming detector, SATCOM security, integrated modular radio, GNSS communication, and secure ATC communication.

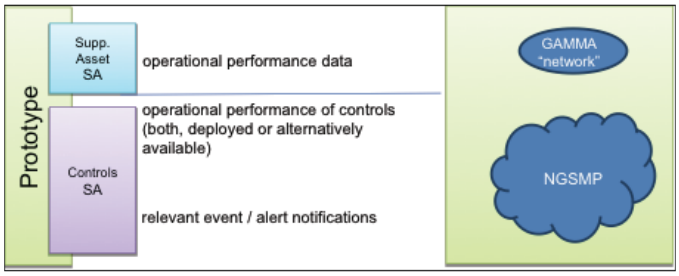


Figure 3 – GAMMA Principal Information Relationship

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:

- S*ecurity 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*	*Likelihood*	*Risk Level*
Voice system	*False ATCO*	*Arrival management, landing procedure*	*5*	*4*	*High*
		Departure management, take-off procedure Conflict management			
		Conflict management			

Table 1 Example of Risk level Evaluation

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_05	*Voice System*	*Each ACC/TWR shall operate and control speaker verification.*
ASC_TFA_05	*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

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

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 chall enging 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:

o Identification of the restricted data/information: sensitive and confidential data/information.

o 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).

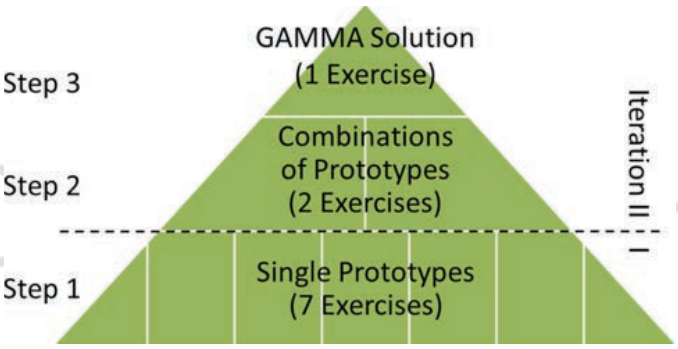


Figure 6: Validation Process Approach

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: Security requirements realized by 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.-S_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.-S_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.-S_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.-S_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.-S_2	Stress detection module assistance will be accepted by ATCOs
AC_SACom_7	REQ - ATC - 9	Obj.-S_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.-S_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.-S_1	With the SACom prototype stress detection module False ATCOs are detected earlier compared to the baseline
AC_SACom_10	REQ - ATC - 9	Obj.-S_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.-S_2	Speaker verification module assistance will be accepted by ATCOs
AC_SACom_12	REQ - ATC - 10	Obj.-S_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.-S_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.-S_1	With the SACom prototype speaker verification module False ATCOs are detected earlier compared to the baseline
AC_SACom_15	REQ - ATC - 10	Obj.-S_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.-S_2	SACom prototype assistance will be accepted by ATCOs
AC_SACom_17	... REQ - ATC – 9 REQ - ATC - 10	Obj.-S_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.-S_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.-S_1	With the SACom prototype False ATCOs are detected earlier compared to the baseline
AC_SACom_20	... REQ - ATC – 9 REQ - ATC - 10	Obj.-S_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.

EMAIL ADDRESSES

patrizia.montefusco@leonardocompany.com

rainer.koelle@eurocontrol.int

racasar@isdefe.es

tim.stelkens-kobsch@dlr.de

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

SECURITY SITUATION MANAGEMENT – DEVELOPING A CONCEPT OF OPERATIONS AND THREAT PREDICTION CAPABILITY

***Denis Kolev**, Rinicom, Lancaster (United Kingdom)*
***Rainer Koelle**, Lancaster University, Lancaster (United Kingdom)*
***Rosa Ana Casar Rodriguez**, Isdefe, Madrid (Spain)*
***Patrizia Montefusco**, SELEX, Napels (Italy)*

ABSTRACT

This paper addresses a collaborative security situation management capability for air navigation. In particular, we formulate the development of a threat prediction capability as a situation management problem mapping the concepts of situation awareness and information fusion. Air transportation and air navigation is undergoing a fundamental transformation. This also requires novel approaches to system security and the management of security incidents across a network of actors. The Global ATM Security Management project addresses this problem space. The work reported in this paper, conceptualizes a security function that supports the management of security incidents on a local, national, and regional level supporting the collaborative effort of classical air traffic management stakeholders and security stakeholders. The security function is based on a network of distributed nodes and capabilities. One such a capability is the threat prediction model. This component is based on a representation of the (sub-) system context as a network of supporting assets, event detection sensors, and associated security controls. Based on the description of the (sub-)system context as a sequence of situations, the threat prediction capability addresses the identification of a security incident and its potential impact as an optimization problem. This paper reflects the work of the first year of the project. In particular, it demonstrates the general feasibility of the approach and the further modelling and preparatory work for further validation activities.

INTRODUCTION

From the beginning of the 21st century, aviation has been undergoing a continual transformation with novel technologies being readied for deployment in ground-based, airborne and space-based systems. Throughout the past decade, the security of the air navigation system has become more prominent [1]. Today, efforts are ongoing to embed security risk management into the overall system engineering approach in air traffic management system development. However, the political goals and priorities for transformation programs like SESAR and NextGen put a strong emphasis on the early deployment of operational concepts and technological enablers with little focus on the identified security threats and emerging vulnerabilities stemming from these developments.

One particular research gap is the lack of a system-wide collaborative security function to support the decision-making in terms of security across the different air navigation system stakeholders. The Global ATM Security Management (GAMMA, http://www.gamma-project.eu/) project, funded under the 7th Framework Program of the European Commission, stems from the growing need for targeted research in addressing this capability gap.

Initial work on a collaborative security capability has been conducted as part of pan-European research projects, for example, SAFEE – Security of Aircraft in the Future European Environment, PATIN – Protection of Air Transportation and Infrastructure, and ERRIDS – European Regional Renegade Information Dissemination System, an initial NATO/EUROCONTROL demonstration project. Similar research efforts have been reported in the United States [2]. However, the results are not carried forward under the umbrella of the on-going transformation programs SESAR and NextGen.

The GAMMA approach builds on the opportunities opened by a collaborative framework for managing security. The project activities flow from a comprehensive security risk assessment enabling the definition of requirements and architecture components for a comprehensive set of security capabilities in the future air navigation system [3].

This paper addresses a collaborative security situation management capability for air navigation that allows for the dynamic identification and assessment of security threats, and the coordination of security measures. The security function is formulated as a situation management problem and the associated threat prediction capability

is based on a network of security information nodes formed by the air navigation system components. Both modelling approaches support a deployment strategy for such a security capability in future air traffic management contexts like SESAR and NextGen that are complementary to current developments and can be easily embedded.

This paper is organized as follows: Following this introduction, a short overview of the state of ATM security is given. The third section introduces the modelling approach. Next, the threat prediction capability is described. Then a short discussion of our results is presented. The paper closes with conclusions and recommendations for further work.

BACKGROUND – STATE OF ATM SECURITY

Operational Risk Assessment and Emerging Regulatory Requirements

Operational risk assessment is not a fundamentally new approach in aviation or air traffic management. However, the classical approach to operational risk encompassed the concept of safety and the identification of system-inherent risks (e.g. human error, technical reliability). Security considerations were primarily focused on contributions of the air navigation system to national security and defense.

In the aftermath of September 11th 2001 and major outages of public services (e.g. electricity grip, public transportation), increased efforts were undertaken in the identification of adequate security measures and the protection of critical infrastructures. Within this context the criticality of the air navigation system has been confirmed and service providers have been mandated to implement security management systems.

In Doc 9854, ICAO defines the expectation for air navigation security as one of the eleven key performance areas [4]. In the European Context, the European Commission adopted this requirement in the Single Sky Regulation (i.e. EC Reg. 2096/2005, 1035/2011) and ECAC included a recommendation on ATM Security in Doc 30. EUROCONTROL in close collaboration with its stakeholders developed an initial ATM domain-dependent Security Management System and Security Risk Assessment Methodology as principal guidance in this field. This initial work served as an input to the SESAR Definition and Development Phase and the recently developed ICAO Manual on ATM Security, Doc 9985 [5].

Current Developments

In Europe, SESAR is now moving into the deployment phase. In June 2014, the European Commission adopted implementing regulation IR716/2014 identifying six air traffic management functionalities to be deployed by a specific date. The associated implementation plan is established and managed by the newly created SESAR Deployment Manager (SDM). The SDM released its Deployment Programme Version 1 in June 2015 defining 44 families of implementation projects and their priorities for the 2014-2020 time horizon [6].

Though the SDM program recognizes the relevance and role of security, little effort has been undertaken to embed security into the system-development life-cycle or require a specific security function or supporting capabilities. References to security are typically on the technological level. For example, the SDM Deployment Programme vaguely requires security measures for

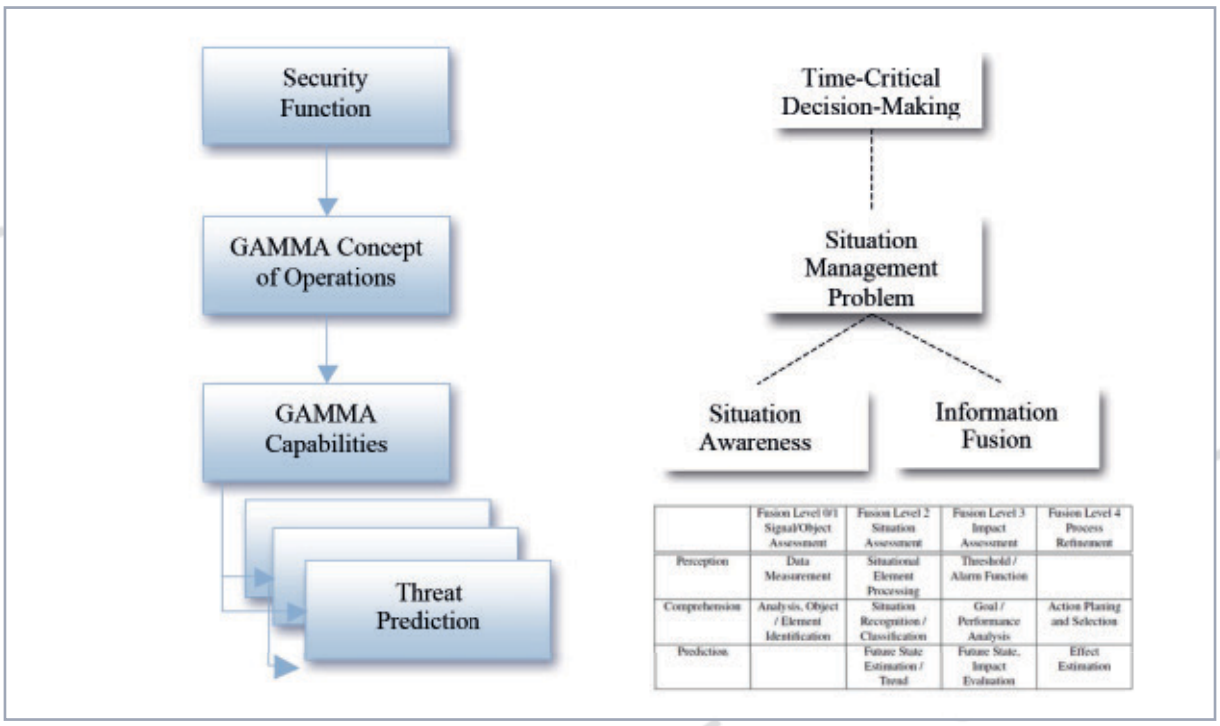


Figure 1: GAMMA Problem Space Mapping

certain projects with a view to ensure continuity of system operations.

GAMMA Project

The lack of a security function and its thorough implementation across the air navigation system and the current transformation programs has been identified by other research (c.f. above). GAMMA addresses this void and is designed to develop solutions to emerging security vulnerabilities of air navigation and provide validated proposals for the implementation of these solutions.

The GAMMA project stems from the growing need to address security threats to air traffic management / air navigation in a consistent manner. The security solutions proposed by GAMMA build on the principles and concepts related to security management in a collaborative multi-stakeholder environment. The proposal emerges from a detailed assessment of ATM security threat scenarios carried out in full compliance with SESAR methodologies and building on its results [3].

In that respect, GAMMA fills the void and complements SESAR, with a concrete proposal for the operational use of innovative technological enablers establishing an ATM security function as an additional service in the air navigation system.

MODELLING THE SECURITY FUNCTION

Figure 1 depicts the modelling approach employed in this paper. In particular, we describe the security function of the air navigation system as an application of time-critical decision-making. The subsequent situation management problem is then described by the functions, modes of operations, and supporting capabilities of the GAMMA concept of operations. In this paper, we discuss one of the GAMMA capabilities, i.e. the threat prediction, as a mapping of two situation management concepts: situation(al) awareness and information fusion.

Air Navigation System Security Function

During the preparatory work for the SESAR Definition Phase, a novel definition for the term ATM Security emerged as it was recognized that the classical understanding of aviation security and the associated primarily supporting role of air navigation did no longer meet the future requirements. 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

2. collaborative support to other aviation system stakeholders.

This definition allows for a first conceptualization of an ATM Security Function (c.f. Figure 2). 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.

This paper refers to function as the operational, procedural, and technical means to realize a desired 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 internal security actors.

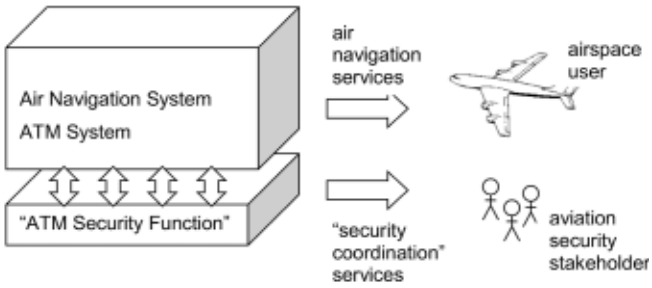


Figure 3: Security Function Concept

GAMMA Concept of Operations

The overall purpose of the GAMMA project is to demonstrate a comprehensive approach to ATM security by providing a concrete proposal for the implementation of capabilities to address and manage security risks in a dynamic and collaborative multi-stakeholder context (i.e. GAMMA organization). This requires for

1. self-protection / resilience of the ATM system

• the dynamic operation of the day-to-day management of the established security (sub-) systems through the provision of monitoring and analysis capabilities; and

• the handling of security incidents across the complete spectrum from identification, decision-making / response, and post-incident activities.

2. collaborative support

• the provision of appropriately sanitized data/ information in support of the aviation security mission of the respective stakeholder; and

• the support to aviation security response by ensuring the mission requirements in terms of separation and synchronization of air traffic, and provision of incident support related information.

The security function conceptualized by GAMMA is a network of GAMMA operators and users, including local security (sub-)systems or system security functions, representing a network of distributed nodes embedded within the air navigation system. Next to this organization and set of technical functions, the GAMMA concept builds on a tailored information exchange between the different nodes on three principal levels:

- local – local security (sub-)systems or component embedded in the ATM/CNS infrastructure or a specific local GAMMA security operation center supporting the integration of local level information with GAMMA network wide information and support functions;
- national – the national reporting center for a set of local GAMMA security operations centers. This level may be provided with additional control capabilities for the continuous dynamic security management which are not available on local level or complement the local level; and
- pan-region/European – pan-regional reporting and coordination (e.g. European GAMMA Coordination Center).

Figure 3 presents the security situation management network for a generic four state context and how this context can be conceptualized forming a network of distributed nodes embedded in the current air navigation system context.

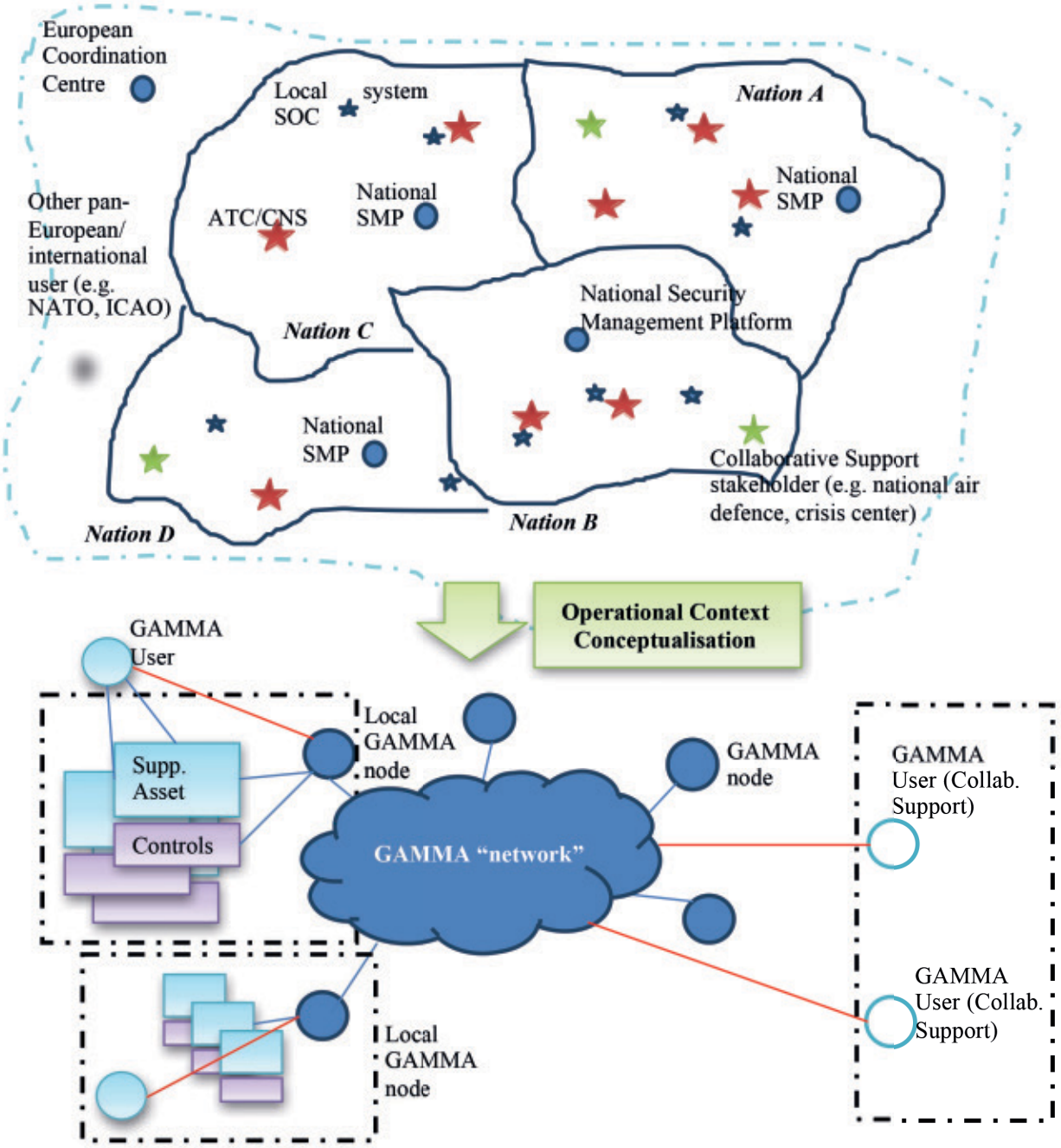


Figure 4: GAMMA Security Situation Management Network

Security Situation Management

Situation Management is an emerging paradigm. Jakobson et al (2005) introduces the term 'Situation Management' as collectively identifiable operations revolving around situation monitoring (sensing), awareness (reasoning), and control (acting) in dynamic and operational environments [7]. Alfredson (2007) stresses the process of managing dynamic situations by combining internal and external resources throughout the sense-reason-action cycle [8]. These concepts are combined by conceptualizing situation management as a distributed decision-making and multi-agent problem based on an information-centric approach suitable for situation analysis and resource- and action-management [9].

Situation(al) Awareness

One key aspect of the situation management approach is the establishment of situational awareness coordinated and shared across the different collaborating actors. The Endsley model is the predominant model in the situation(al) awareness literature [10][11][12]. Conceptually, the Endsley model describes the human decision-making process within (safety-) critical decision-making contexts (e.g. aviation). The Endsley model defines Situation(al) Awareness as "[t]he perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." [10] With this definition three separate layers of situational awareness can be distinguished: 1.) perception, 2.) comprehension, and 3.) prediction.

Ae we place our research into the time-critical decision-making domain, we can immediately postulate these situation(al) awareness layers as functional requirements on the GAMMA security solution.

Information Fusion

Due to the multi-disciplinary nature of fusion and its broad application, fusion has been researched and described from a variety of perspectives. There is some ambiguity in the terminology used in the fusion literature. Various researcher use the terms 'data fusion', 'information fusion', 'sensor fusion', 'multi-sensor data fusion', etc in an interchangeable manner, while others apply subtle differences. Recent research defined information fusion as the umbrella term: "Information fusion is the study of efficient methods for automatically or semi-automatically transforming information from different sources and different points in time into a representation that provides effective support for human or automated decision making."[13]

The dominant model used within the data fusion community is the JDL Data Fusion model; this defines a stepwise refinement of information [14]. The JDL however is a functional model, which means it does not itself describe how this information refinement is made. The current emphasis is towards a generalization of sensor fusion into so-called higher-level information fusion (HLIF). Recent work in HLIF concentrates on large dynamic sensor networks and higher-level information fusion [15], with a focus on the identification of objects, events and their relations.

The act of fusion serves to enrich the data / information. Fusion can serve different purposes; for example the fused information is of higher accuracy, reduced uncertainty, richer / completer. In that respect fusion serves to refine or expand our knowledge, information or beliefs about the real world [16, 17]. The processing, collection and combination of information is an essential step in time-critical decision making and the portrayed situation management approach.

	Fusion Level 0/1 Signal/Object Assessment	**Fusion Level 2** Situation Assessment	**Fusion Level 3** Impact Assessment	**Fusion Level 4** Process Refinement
Perception	Data Measurement	Situational Element Processing	Threshold / Alarm Function	
Comprehension	Analysis & Object / Element Identification	Situation Recognition / Classification	Goal / Performance Analysis	Action Planning and Selection
Prediction		Future State Estimation / Trend	Future State & Impact Evaluation	Effect Estimation

Table 1. Mapping of Situation Awareness and Data Fusion Levels

GAMMA demonstrators

The GAMMA project revolves around the demonstration of the GAMMA solution through a set of validation exercises. The demonstrators form part of the aforementioned functions and sub-systems that may be embedded in the ATM/CNS system context. In that respect, some of the GAMMA demonstrators reflect security enriched prototypes for ATM/CNS system components (i.e. supporting assets from a security risk assessment perspective). GAMMA will conceive solutions 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.

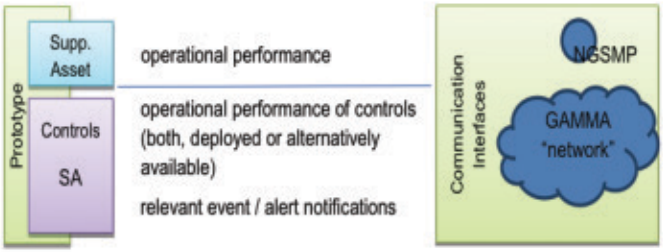


Figure 5: GAMMA Information Concept

Following the distributed security situation management network concept, these demonstrators will provide situational information on their operational status, the operational performance of their security controls, and relevant event and event information via the GAMMA network to the respective functions within the GAMMA solution context (c.f. Figure 4).

THREAT PREDICTION CAPABILITY

The threat prediction capability is a decision support system function and hence represents a node in the distributed GAMMA security situation management network. The aim of the threat prediction capability is to process and analyze situational information received from other nodes, and establish a prediction for the actions of an adversary, including a rough assessment of the – expected – impact. The key functionality is based on the correlation of information from diverse data sources under the assumption of high false positive "alarm" rates. The threat prediction capability outputs associated alerts and threat levels, lists of potentially vulnerable supporting assets, and attack success.

Within the current GAMMA concept of operations, the threat prediction capability is envisaged as a potential local security sub-system function primarily working on sensor feeds from local sensors (e.g. event detection). On a national level, the capability may be embedded within the national security management platform. In this context, it will process information from various local systems and addresses the security situation on a higher than system component level.

In general, the threat prediction capability is based on a model of the system context. This model is built on deployment and initialized by describing all possible threats within the modelled (sub-)system through a graph structure. This includes the respective security controls and sensors in place. In that respect, security controls are assigned to the nodes of the graph (i.e. protected asset). Following the model initialization, the capability will process the information received from the sensors and interconnected security (sub-)systems. On the basis of this dynamic input, the internal state of the model is updated. Given that a possible threat is evaluated as likely based on the internal state update, the model evaluates the possible impacts of the anticipated attack mode including targeted supporting asset.

The model is constructed on the basis of a graph structure, i.e. threat path graph *G = (N,A)*. Supporting assets are referenced by a subset of nodes in the graph, $V \subset N$.. Points describing the possible start of potential attacks, i.e. threat entry points, are defined as a subset of nodes $T \subset N$. Each node in G defines a condition/ configuration of the attacker resources, e.g. position, resource availability). Each edge in the graph defines the possible transition from one threat path node to another. Entry points denote possible pre-conditions of the attack. An attack scenario is formalized as a path *P* in the graph *G* from an entry point ($\in T$) to the respective supporting asset $SA \in N$ and the given type of the attack A, performed on SA, formally (*P,A*).

The principle of this formulation is depicted in Figure 5. For each depicted supporting asset also the type of security control and event detectors is encoded in the graph.

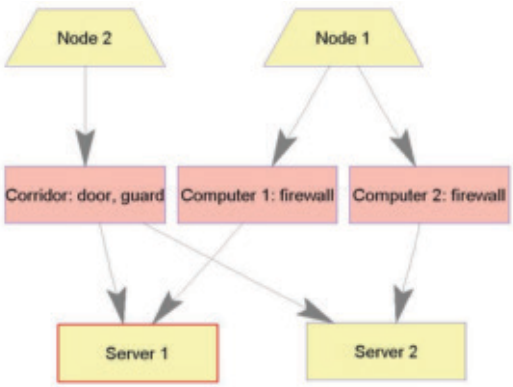


Figure 6: Threat Prediction Capability Graph

Through fusion of the sensor and event detection information it is possible to estimate the skill of the adversary. The skill level characterizes the competence level of the attacker which may be used to evaluate the effectiveness of already deployed security controls. This allows for the support to decision making as a decision to deploy additional security controls to overcome potential vulnerabilities of the controls and appreciate the possible impact after a successful attack. In that respect security controls can be categorized with a skill threshold that defines the minimum skill level an attacker requires to overcome the security control.

The mathematical formulation of the threat prediction algorithm is given as follows. An attack is formalized as a path P in graph G and its type of attack A. Let's assume a probability distribution over (P, A) - p . An event detector placed at node $n \in N$ is denoted by D n . Event detectors are characterized by their false positive detection rate $P_{TP}(n)$ (i.e. the probability of an alarm in case of no event / attack) and their false negative detection rate $P_{FP}(n)$ (i.e. no detection in case of an adversary passing through the node). The event detection information received from a sensor at node n at time t is denoted by d_n^t. Each moment of time t a set of event detections is received $S_t = \{d_{n_1}^t, \ldots, d_{n_{k_t}}^t\}$. describing the perceived signals refining the overall situation. The model assumes a discrete time basis.

The skill level of an attacker (i.e. level of compσσetence) is characterized by the "skill" variable $s \in \mathrm{R}^+$. Each security control for each node is described by "skill" threshold. The adversary is able to overcome the security control, if the skill is higher than corresponding "skill" threshold.

Formally, the prediction task is defined as an estimation problem for p, s given the characteristic sequence S_t , the parameters of the event detectors (i.e. $P_{TP}(n)$ and $P_{FP}(n)$), and the graph structure.

In order to frame the estimation problem, we define a probabilistic graphical network over the variables of the system. Variable s is assumed to be distributed normally $N(s|\mu\ \sigma)$, where $\mu\ \sigma$ are the corresponding mean and variance. We add auxiliary variable t, which denotes the threat selected by the adversary. $t \sim p$, and p defines the distribution of the variable t. The probability of the event detection is then given by the selected path and "skill" and is denoted by $p(d_n|s, t)$. It is equal to $P_{FP}(n)$ if node n does not belong to the path defined by t or if the "skill" of the adversary is not enough to reach node n using path defined by t. Otherwise the probability of detection is equal to $P_{TP}(n)$. Detections in S_t are assumed to be iid.

Given, $S_t, p(s)$ and $p(t)$ we aim to estimate $p(s|S_t)$ and $p(t|S_t)$. This problem could be solved using approximate Bayesian inference. Thus, at each moment of time, the distributions of s and t are updated. These updates are used to identify the existence of the adversary, his intention, and the level of competence. This allows for the prediction of potential impacts on the system.

DISCUSSION

Results from the GAMMA project have been discussed and presented during dedicated GAMMA user-group meetings and related security stakeholder meetings. The results so far demonstrate the general feasibility of the GAMMA solution and provide tangible input in the further refinement and development of the GAMMA prototypes. In this section, we focus on the main aspects of this paper.

Concept of Operations

The GAMMA user-group meeting in autumn 2014 supported the refinement of the GAMMA security risk assessment, threat scenarios, and GAMMA architecture model. A major discussion revolved around the different modes of operation (e.g. local security activities versus national policies) before, during, and in the aftermath of an incident.

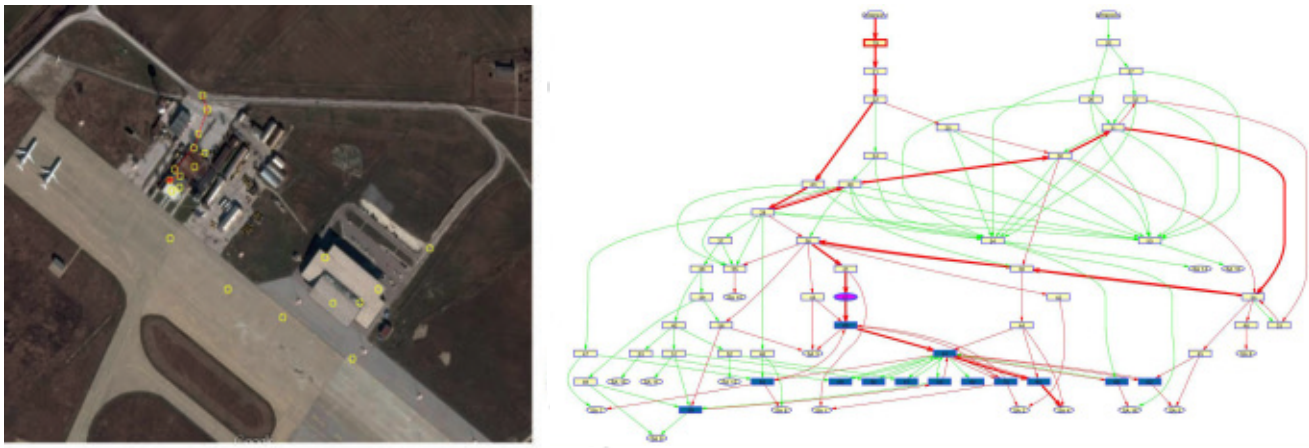


Figure 7: Threat Capability Demonstration

One of the key stepping stones in developing the GAMMA concept of operations was the move from a classical security risk management and architecture description to a security situation management model (c.f. above). The confirmation of the building blocks through relevant previous research, the initial work of GAMMA, and the user-group feedback allowed for the conceptualization of the GAMMA solution as a network of distributed nodes collaboratively managing the security of the air navigation system.

The GAMMA concept of operations offers a valuable input to the further development of the validation scenarios identifying the relevant information processes between the different actors (i.e. GAMMA operators and users) and functions (e.g. information dissemination system, threat prediction capability, local security (sub-) systems, and GAMMA prototypes).

Threat Prediction Capability

The threat prediction capability has been recently showcased at the EUROCONTROL/NATO ATM Security Workshop (June 2015). The demonstration revolved around a local scenario at an aerodrome. The subsystem components and controls were modelled by approximately 80 nodes (c.f. Figure 6).

With this model and approach, we are able to bridge the situation awareness concept and data fusion concept (c.f. Table 1). In particular, the proposed threat prediction is mostly related to Fusion Level 3. According to the description of the threat prediction capability, it requires aggregated information characterizing the state of each of the system nodes. Lower level processing (level 2) may enhance the prediction performance, but it may involve significantly different kind of analyses (e.g. statistical streaming data processing, expert-based classification) which are strongly related to the specifics of the analyzed sub-system. Therefore, from a system-level point of view, level 2 data analyses may be easily "encapsulated", so that alarm generation processes (level 2) and alarm correlation/threat prediction processes (level 3) are separated in a natural manner. The latter support the incremental implementation of the threat capability and iterative deployment of the GAMMA information concept (c.f. Figure 5) within the current or future air navigation system context.

CONCLUSIONS

This paper presented our approach to devise a concept of operations for GAMMA and develop an associated threat prediction capability for a security function embedded into the air navigation system. We describe this capability as a collaborative security situation management problem. Our present work has focused on the fundamental design aspects and underlying theory for the development of the concept of operations and the subsequent development of an initial threat prediction capability. The GAMMA threat prediction model / initial capability has been successfully demonstrated at a recent stakeholder workshop on ATM Security. As part of the GAMMA work program work is ongoing to integrate the threat prediction capability with other GAMMA demonstrators, ultimately enriching the coverage of sensor measurements and processed information in support of enabling GAMMA operators to collaboratively manage a security situation.

The results presented in this paper help to show the general feasibility of the security situation management approach expressed through the GAMMA concept of operations. While the concept of operations is wide enough to capture the generic context of air navigation, it must be recognized that the GAMMA activities target a subset of the security function. Nevertheless, the GAMMA solution builds on SESAR in such a way that the demonstrators could be easily embedded in the future ATM/CNS context.

The concept and capability presented in this paper mark the mid-point of the GAMMA project. This allows for a wider discussion of the project deliverables and a subsequent refinement to fully meet the project goals and address stakeholder requirements in terms of security capabilities. As part of the on-going activities a GAMMA security information exchange model is developing and will be further reshaped as part of the future work to enable the information exchange between the different GAMMA nodes and air navigation system components.

This paper described the principle initialization and operation of the threat prediction capability. One aspect that needs further attention is the fact that sensor and event detector may produce false read-outs or alarms, or that the event detector may not detect the adversary / method of attack. Another aspect is the temporal variation in the security control configuration. For example, controls considered during the initialization stage may degrade over time or are deactivated for maintenance reasons. Such dynamic variations of the configuration and the reliability of the sensor and detection feeds require a further refinement of the threat prediction capability modelling approach.

REFERENCES

[1] Koelle, R., G. Markarian, and A. Tarter, 2011, Aviation Security Engineering, A Holistic Approach, Norwood, MA, Artech House.

[2] Koelle, R. and Tarter, A. (2012) "Towards a Distributed Situation Management Capability for SESAR and NextGen", Integrated Communications, Navigation and Surveillance Conference (ICNS 2012), pp.O6-1-O6-12.

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

[4] International Civil Aviation Organization (ICAO), 2005, Doc 9854, Global Air Traffic Management Operational Concept, First Edition, Montreal, ICAO..

[5] International Civil Aviation Organization (ICAO), 2012, Doc 9885 AN/492-Restricted, Air Traffic Management Security Manual, Montreal, ICAO.

[6] SESAR Deployment Manager, 2015, Deployment Programme, Version 1 (DP v1), Work Package B2 – 4.1, Deliverable 4.1.3, Brussels.

[7] Jakobson, G., Lewis, L., Matheus, C., Kokar, M., and Buford, J. (2005) "Overview of Situation Management at SIMA 2005", Military Communications Conference, 2005. MILCOM 2005. IEEE , vol.3, pp.1630-1636.

[8] Alfredson, J. (2007) Differences in Situational Awareness and how to manage them in the development of Complex Systems, PhD Thesis, Linköping University.

[9] Koelle, R. (2012) A Study into Situation Management applied to Time-Critical Decision-Making in Aviation Security, PhD thesis, Lancaster University.

[10] Endsley, M. R., 1995, Measurement of situation awareness in dynamic systems. Human Factors, 37, pp. 65–84.

[11] Endsley, M. R., 1995, Toward a theory of situation awareness in dynamic systems. Human Factors, 37, 32–64.

[12] Wickens, C. D., 2008, Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement, Human Factors, Vol. 50, No. 3, pp. 397–403.

[13] H. Boström, S. F. Andler, M. Brohede, R. Johansson, A. Karlsson, J. van Laere, L. Niklasson, M. Nilsson, A. Persson, and T. Ziemke, 2007, On the definition of information fusion as a field of research. Technical report, University of Skovde, School of Humanities and Informatics, Skovde, Sweden.

[14] Llinas L., 2004, Revisiting the JDL Data Fusion Model II, proceedings FUSION04, Stockholm, Sweden, pp. 1218 – 12130.

[15] Scott P.D. and G.L. Rogova, 2004, Crisis Management in a Data Fusion Synthetic Task Environment, 7th International Conference on information Fusion, Stockholm, Sweden.

[16] E. Blasch, I. Kadar, J. Salerno, M. Kokar, S. Das, G. Powell, D. Corkill, and E. Ruspini, 2006, Issues and challenges in situation assessment (level 2 fusion). Journal of advances in Information Fusion, I(2).

[17] E. I. Bloch, A. Hunter, A. Ayoun, S. Benferhat, P. Besnard, L. Cholvy, R. Cooke, D. Dubois, and H. Fargier. 2001, Fusion: general concepts and characteristics. International Journal of Intelligent Systems, 16: pp. 1107–1134.

ACKNOWLEDGEMENTS

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

DISCLAIMER

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

EMAIL ADDRESSES

denis.g.kolev@gmail.com

rainer.koelle@eurocontrol.int

racasar@isdefe.es

pmontefusco@sesm.it

34th Digital Avionics Systems Conference
September 13-17, 2015

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.

GAMMA CONOPS

A New Vision for AMT Security Management

PRINCIPLES AND BACKGROUND FOR THE GAMMA SOLUTION

The ATM Security solution proposed by GAMMA builds on the principles and concepts related to Security Management in a collaborative multi stakeholder environment, while maintaining a strong link to the current international and European legal framework and the constraints given by the respect of national sovereignty.

Security is a national responsibility which cannot be delegated. This principle has been highlighted in ICAO Annex 17 as well as in the Implementing Rule 1035/2011 of the Single European Sky legislation, which recognises the role of the State in security governance, requiring the implementation of a security management system and the establishment of a first level of coordination to discharge the institutional responsibility for national security.

The GAMMA solution has been defined and developed with these principles in mind and aims at facilitating and enhancing the implementation of a Security Management system by extending the scope of collaborative support beyond the local level.

The GAMMA vision recognises the opportunities opened by a collaborative framework for managing security, building a solution based on the self-protection and resilience of the ATM system with an immediate relevance to the real security challenges facing the existing ATM environment and its evolution foreseen in SESAR.

The proposal emerges from a detailed assessment of ATM security threat scenarios carried out in full compliance with SESAR methodologies and building on its results. The solution outlined here should therefore be seen as complementing the work performed in SESAR, with a concrete proposal for the operational use of innovative technological systems establishing an ATM security function as an additional service in the Air Navigation System.

GAMMA SOLUTION

The operational and technical scope of the GAMMA vision is given by the existing ATM system and its evolution foreseen within SESAR. The GAMMA solution can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.

GAMMA establishes three different levels for managing security:

- the **European** level represented by the European GAMMA Coordination Centre (EGCC),
- the **National** level represented by the National GAMMA Security Management Platform (NGSMP)
- the **local** level represented by local security systems as well as Local GAMMA Security Operation Centers (LGSOC).

Two different human roles are considered within the GAMMA concept:

- GAMMA Operators, represented by actors performing functions within the LGSOC, NGSMP and EGCC
- GAMMA Users, represented by Users of the local security systems.

The picture below depicts the main parts of the GAMMA solution and their interactions. It represents how GAMMA is proposing to manage ATM security.

The GAMMA solution is designed for seamless adaption and integration into the local ATM systems. For this reason the local level is represented by two types of solutions:

- Local security systems embedded in the current or future ATM systems (and/or procedures) that address security aspects operating independently from the LGSOC.
- A specific GAMMA system (LGSOC) with access to the information defined within GAMMA to support the local security activities.

When introducing the GAMMA solution into the ATM environment the local security systems may provide security information to the LGSOC or directly to the NGSOC (for example, alerts, monitoring of supporting assets, monitoring of security controls/countermeasures, etc).

The LGSOC is an information sharing platform introduced into the ATM environment by the GAMMA solution, with the aim of collecting and processing security information from local security systems as well as receiving and

providing information from the National and European levels. The LGSOC therefore provides a local GAMMA operator with a window towards the information elaborated by GAMMA at National and European level through an extended collaboration platform. The GAMMA architecture is open to local implementations and the existence of LGSOC is not mandatory as local security systems could be interconnected or linked directly to the NGSMP.

The **National level** will have the capability of processing and analysing the information received from the lower level through the operation of an information sharing platform (NGSMP) allowing the detection and prediction of attacks as well as proposing the corresponding alerts, actions or countermeasures and predicting corresponding impacts.

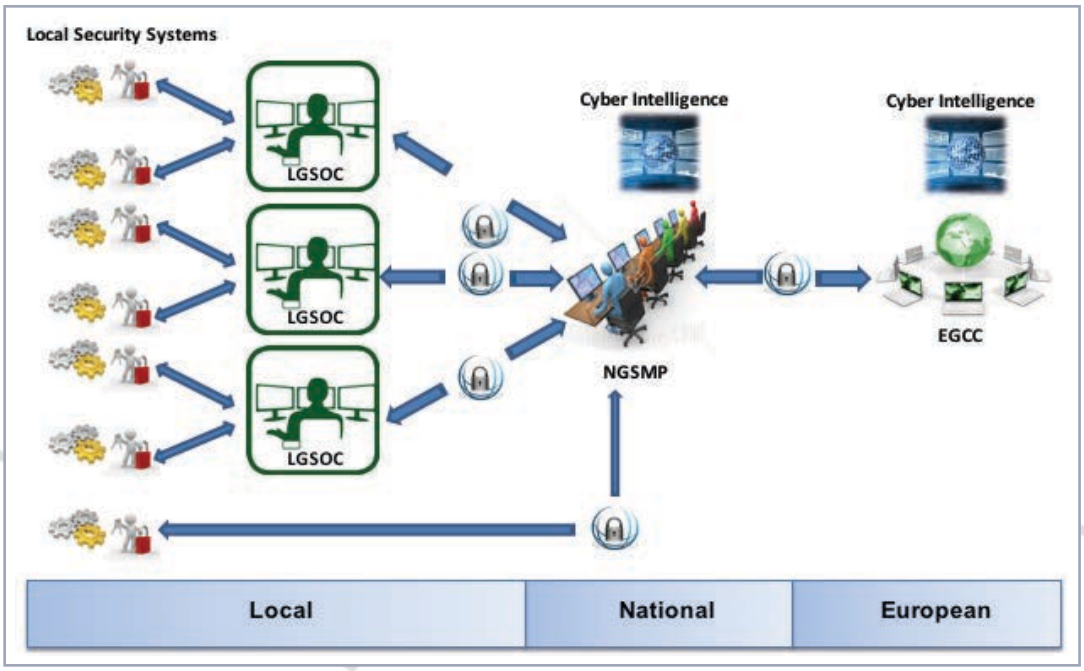
The above described opportunities made possible by the establishment of a cooperative environment highlight the need for an appropriate 'sanitisation of information' in order to encourage the exchange of information within the legal limits set by the regulatory framework. Sanitisation should be seen a prerequisite for the successful exploitation of collaborative environments within the existing regulatory framework.

Sanitisation of the information aims to categorize the sensitive information, generated at local and national level that can be disseminated at European level, if necessary opportunely modified so as to eliminate sensitive aspects. In the picture above the padlock symbol represents where the sanitization process can be performed.

The **European Level** (EGCC) will enrich the opportunely sanitized information derived from the National level extending the cooperation platform through the operation of Cyber Intelligence functionalities in order to discover possible external threats related not only to the ATM environment but also to other services/systems whose disruption or destruction could cause domino effect on ATM. The EGCC will then be responsible for feeding such information to the NGSMP for further disseminating to the local levels.

The GAMMA solution therefore opens the way for the European level to propose (but not enforce) recommendations on actions or measures to be taken at lower levels, in line with existing principles of national sovereignty and responsibilities over security issues. The GAMMA architectural vision therefore enlarges the scope for cooperative management of ATM security while remaining rooted in the fundamental principle that Security cannot be outsourced or delegated.

The GAMMA Solution has been conceived as a concrete and easily deployable proposal for the management of ATM security, exploiting innovative technologies and procedures while maintaining compatibility with the European ATM framework defined in the Single European Sky.



Civil and Military Cooperation Issues

Airbus DS

GAMMA is conducting a thorough assessment of the ATM Security framework with the aim of identifying the institutional environment within which the GAMMA proposed solution is intended to operate so as to allow for its smooth adaptation and integration into this environment. As part of these studies, all aspects of cooperation and coordination between the civil and the military for ATM Security purposes are considered, including governance, organisation, procedures, regulations, technologies, joint civil-military training and exercises related to incident/crisis management.

The military are involved in ATM security in two ways [1]:

- for self-protection of the ATM system; providing necessary support on request of civil aviation authorities and ANSP or Airports Operators for the protection of their facilities (normally in case of raised security alert levels);
- for collaborative support; defining the information and support requirements needed from ANSPs, Aircraft Operators and Airport Operators, for air defence, contingency and incident management situations.

As part of the GAMMA study into these issues, the following approach has been followed:

- the 'as-is' (current) situation of the civil-military cooperation in ATM security has been established through questionnaire replies from military organisations of different European countries and subsequent meetings with these organisations;
- from this 'as-is' situation, a set of best practices has been identified;
- finally, a list of improvements is proposed to enhance the civil-military cooperation in ATM Security.

Two major types of threats are considered:

- **Airborne threats**, covering various situations of airspace security incidents (including hijacking and renegade situations), where the military have a leading role in the resolution of the incident, with the support of ATM. The scenarios using drones ("RPAS") are also included.
- **Technological threats**, where the ATM systems or assets are targeted and the military play a role first by self-protecting their own systems connected to ATM systems and in some cases by providing air navigation services (contingency planning) or performing post-incident analysis. The military also play a growing role in the threat assessment phase regarding cyber-security.

The improvements identified by GAMMA in this study are of different natures and can cover different horizon times.

Among the improvements of technological nature, one can note the following ones:

- Use of SESAR Dynamic Mobile Areas (DMA's) for airspace security purposes
- Use of existing Safety Nets for Security Nets
- Exchange of ATM incident-related information between civil and military via data link
- Use of future Global Aeronautical Distress & Safety System (GADSS) for airspace security purposes allowing early warning of airspace security incidents (this improvement could be coupled in the longer term with aircraft passivation).

Among the improvements of operational or organisational nature, one can note the following ones:

- Harmonisation of ASSIM (Airspace Security Management) Implementation between nations
- Upgrade of agreements between neighbouring National Governmental Authorities to better handle cross-border situations
- Full involvement of the military in the definition and update of the ATM Security Policy

Regarding the training aspects the following improvements are suggested:

- Joint Civil/Military Training exercises on technological and airborne threats based on distributed simulator platforms
- Introduction of new types of training exercises on cross-border airspace security incidents (such as the case of a business aircraft hidden behind a commercial aircraft)

REFERENCES

[1] As defined in ICAO Cir 330 AN/189, EC Regulation N° 1035/2011 and EUROCONTROL Manual for National ATM Security Oversight.

The Social Acceptance of the Passivation of Misused Aircraft

***Ana P. G. Martins**, Institute of Flight Guidance, Deutsches Zentrum für Luft- und Raumfahrt e.V., Braunschweig, Germany*

ABSTRACT

One procedure under consideration to handle the threat posed by misused aircraft is passivation. In a passivated aircraft no more inputs from the cockpit are accepted and the aircraft safely lands in the nearest suitable airport without intervention from the pilots. Aircraft passivation is a procedure to be used in an emergency situation and would be handled as such by all stakeholders (air traffic control, airports, airlines, etc.). This paper attempts to address for the first time the social acceptability issues faced by passivation. It is assumed that the introduction of such a system in aircrafts will be a contentious issue expected to be met with strong resistance by pilots and the public in general. In this paper some of the technology under consideration is presented. This is followed by a discussion of the acceptance of similar technologies (unmanned aerial systems, driverless cars) before the social acceptance of passivation is discussed in more detail. Among the recommendations is the need to raise public awareness and familiarity with the technology. Pilots' acceptance is also seen as essential. Once society trusts the technology behind the system and the risks are deemed small enough, acceptance of passivation under some specific conditions should be possible.

Keywords: passivation; social acceptance; misused aircraft

INTRODUCTION

This paper summarizes a concept study being done in GAMMA, an on-going FP7 research project. GAMMA addresses the full set of security threats and vulnerabilities affecting the ATM system and attempts to establish a framework to manage these, extending the scope of SESAR.

Several ATM Security objectives have been identified in GAMMA, among them the need to detect illicit use of airspace (a/c in exclusion zone, without ID or without known flight plan), to detect abnormal situations of identified flights (deviation of flight trajectory or procedure, unlawful interference on-board, renegade aircraft) and contribute to airspace security incident management (contact authorities upon detection of abnormal situation and perform the relevant procedures).

To anticipate and mitigate main threats and risks to ATM, several procedures to the threats described above have been discussed by international organizations (including EASA, NATO) and national authorities. One such procedure is aircraft passivation. In a passivated aircraft all cockpit inputs are disabled and the aircraft safely lands in the nearest suitable airport.

At least three European-wide projects (SAFEE, SOFIA, PATIN) have looked into passivation systems, but mostly discussed the technical issues that need to be addressed before such system can be introduced in aircrafts. A common finding in these projects was the need to address society's acceptance of the passivation system.

A. The need for increased air travel security

In 2012 the air transport industry flew a total of 2.9 billion passengers, corresponding to 31 million aircraft departures [1]. Even though flying is one of the safest modes of transport, the events of September 11, 2001, raised several issues regarding aircraft security and the use of aircrafts to carry out terrorist acts. Ever since, civil aviation security became one of the greatest concerns not only for the industry, but governments and international organizations.

The misuse of civil aircraft is usually associated with hijacking, which traditionally involves the seizing of an airplane to collect some ransom, make certain demands or as a political statement. Before 2001 the crew of a hijacked plane was instructed to cooperate, land the aircraft and let the authorities handle the situation, as this was assumed to minimize the loss of life. The attacks in American soil, however, introduced a new threat: the use of aircrafts as weapons against targets in the ground, with the goal of causing as many casualties as possible. Hijacked airplanes can also be used to propagate biological or chemical agents, or to multiply the effects of the explosion of a weapon of mass destruction on-board. These different kind of hijackers usually act without warning, make no demands and are not open to negotiation, making it very hard for authorities to deal with such a situation. As a result new procedures and regulations were introduced, together with new information dissemination systems. For example, flight attendants and pilots now receive anti-hijacking and self-defense training. The number of air marshals has also

increased dramatically, with an estimated 4000 working in the US Transportation Security Administration in 2013 (actual numbers are classified), from a pre-9/11 number of 33 [2]. Other countries, such as Australia, Canada and India, have also instituted new programs or strengthened already existing ones.

Currently, once an aircraft has been taken by terrorists, the priority is to reduce the number of civilian fatalities not only inside the aircraft but, most importantly, in the ground. Therefore, several countries (e.g., EUA, India, Russia, etc.) have enacted laws allowing the shooting down of hijacked commercial airlines should it be necessary. Needless to say, this is an extremely unpopular decision that no authority wishes to make. In addition, in 2006 the German Federal Constitutional Court ruled against the shooting down of hijacked aircrafts, deciding it was against the Constitution [3]. And even though the European Court of Human Rights has not legislated on the issue, it provides the same rights to life as the German Constitutional law. That is, both deny the right to take life in favor of rescuing others in normal legal conditions, that is, without first declaring state of emergency [3]. Hence the need to consider alternatives, passivation being one of them.

B. When to passivate?

The most obvious situation in which to use aircraft passivation is any September 11 scenario, i.e., with any aircraft hijacked with the intention of crashing it. Passivation can be seen here as the only way to save the aircraft and its passengers as well as to prevent fatalities in the ground and damage to infrastructures.

However, if the technology is installed, it could also potentially be used in other cases where the crew is incapacitated. For example, in 1999 a Learjet 35 suffered a loss of cabin pressure for undetermined reasons and all on-board are thought to have died of hypoxia. The engines eventually ran out of fuel and the aircraft crashed near Aberdeen in South Dakota. Before that happened, military jets intercepted the airplane and if there had been some risk of it falling in a populated area, most probably they would have shot it down. This option involves some risks as well, as the debris can hit people and cause damage in the ground. Passivation might not have prevented the death of the flight crew and passengers, but it would have made it possible to safely land the aircraft.

Another case of crew incapacitation occurred in Greece in 2005 with the Helios Airways Flight 552. In this case the crew also became incapacitated due to hypoxia and the aircraft crashed after suffering a fuel exhaustion only 33 km northwest of the Athens International Airport. Here, unlike in the previous accident, passivation might have saved at least one life, as two hours after ATC lost contact with the a/c, the F-16 pilot following it reported seeing a person entering the cockpit and trying, unsuccessfully, to control the airplane before it crashed.

In the two cases described above, the social acceptance of passivation would probably not be an issue as it would have been the only way to land both aircrafts. But what about those situations where the crew falls asleep or is so engaged in other activities that the pilots do not respond to ATC calls? As an example, in 2009 Northwest Airlines flight 188 did not communicate with ATC for over one hour, despite repeated attempts by the controllers to reach the pilots. The National Transportation Safety Board determined that the flight crew failed to monitor the radio and instruments after becoming distracted by activities unrelated to the operation of the flight. The pilots eventually established communication and landed the aircraft without further incident, but it is possible that passivation would have been activated shortly after all communications ceased.

The probability of the two pilots falling asleep in the cockpit is also a reality. A report by [4] summarized the results of several polls on fatigue carried out by member associations between 2010 and 2012. Depending on the country, 43-54% of the surveyed pilots indicated that they had fallen asleep in the cockpit without informing the other pilot. And in the UK, a third of the pilots said they woke up to find the other pilot also sleeping. In an incident in May 2012 the pilots of an Air Berlin flight requested an emergency landing in Munich reporting extreme fatigue.

In some cases, one can make a strong argument in favor of passivation (hijacking, crew incapacitation), whereas in some others, it is more of a grey area (lack of communications due to cockpit distraction or to unscheduled rest, etc.). The particular cases in which passivation would be used need to be stated, with clear procedures accepted by all stakeholders. Pilots in particular might not accept a system that takes control of the airplane from them while they are busy with other tasks (approved or not). The need for a lack of ambiguity is also of the upmost importance to the public. This and other issues will be further discussed below.

II. EUROPEAN SECURITY RESEARCH PROGRAMS IN AVIATION

The issue of the social acceptance of aircraft passivation does not have a simple answer, as it depends on several of factors. One among them is the public perception of the technology involved and how it would change the way we fly. Therefore, this chapter presents a short description of some European research programs which directly investigated passivation and the new systems envisioned.

The NATO/EUROCONTROL ATM Security Coordinating Group (NEASCOG), was established jointly by the two

organizations to ensure close coordination on ATM security activities in Europe [5]. The group also includes national and international stakeholders (e.g., ICAO, ECAC, EC, EUROPOL, IATA) that have a role in ATM security. One of the main areas of the NEASCOG work programme is to optimize the sharing of civil and military information. The goal is to provide ATM service providers (civil and military), NATO and national air defense units, national government authorities, intelligence agencies, police agencies, aircraft operators, airports and other units playing a part in aviation security, via encrypted links and in real time, with all the information needed to respond to acts of unlawful interference or suspected acts on-board an aircraft [6]. The available information would concern the flight, the route, the passengers and crew, the cargo, the alert state, threat assessment, the progress of the response by states and information handover between states. SAFEE [7], SOFIA [8] and PATIN [9], all to be described next, expect that the passivation system and/or the authorities in the ground have access to such an information dissemination system.

The EU project Security of Aircraft in the Future European Environment (SAFEE) [7] focused on the development of an aircraft decision support system, which would be able to deal with on-board security issues, including hijacking [10]. One of several new systems to be outlined was the On-board Threat Detection System (OTDS), which detects unauthorized access to the cockpit in flight, dangerous materials and goods, and suspicious behavior. Once an alert threshold has been crossed, a signal is sent to the Threat Assessment and Response Management System (TARMS) which has the capability of activating both the Emergency Avoidance System (EAS) and the Flight Reconfiguration Function (FRF) if it detects that the pilots are no longer in control of the aircraft. The EAS automatically takes over to avoid impact with the ground, whereas the FRF allows an automated landing at a secure airport. The EAS also disables all unauthorized inputs to the flight controls and aircraft systems, including electrical circuits, hydraulic systems and engine power.

One topic of concern was the way the new systems would change the interaction between the pilots and the aircraft in normal operations. Airline pilots who were interviewed about the automatic engagement of the EAS by the TARMS expressed concern about the conditions under which those occur. They were not comfortable with a system which could potentially take over control of the aircraft and urged the need for a clear engagement and disengagement philosophy. The acceptability study of the FRF revealed similar concerns. Even if most pilots agreed that such a system would decrease terrorist risk, many showed reluctance in accepting it. As stated in the final report (pp. 28 [7]): “This psychological obstacle needs to be addressed in further studies with proper consideration of the identified concerns”.

The main goal of SOFIA (Safe Automatic Flight Back and Landing of Aircraft) [8] was to advance the work on the flight reconfiguration function (FRF). SOFIA also introduced a new authority, the Ground Security Decision Station (GSDS) at European level, to manage the emergency and coordinate with ATC, airports, ANSP, national authorities, etc.

Three operational solutions were proposed [8]:

- Flight planning with negotiation: The flight plan is generated by the GSDS and transmitted via a secure data link to the FRF. The FRF then needs to check the aircraft status (e.g., fuel left, condition of all relevant systems) and confirm that there are conditions to perform the plan. Otherwise, more information exchange is required. Once the new flight plan is accepted, ATC keeps the traffic away and the GSDS informs the authorities in the ground, including the airport where the aircraft is to land.

- Military aircraft relay: an intermediary step between the other two options. A specially equipped aircraft needs to intercept the hijacked airplane and connect to the FRF in order to ascertain the aircraft condition. This information would then be transmitted to the GSDS and the new flight plan broadcasted to the aircraft via the military jet. This is the most complex procedure and the one that requires the most time.

- Autonomous flight planning: If communications between the aircraft and ground are disrupted the FRF creates and executes a flight plan. ATC can use predicting techniques to anticipate the aerodrome selected by the FRF, a procedure similar to the one used today with an aircraft with R/T failure. The airplane conditions can also be simulated in the ground to anticipate the solution chosen by the FRF. The degree of uncertainty introduced, however, requires giving ATC time to close the affected sector. Therefore, a holding pattern of at least 15 min is necessary. Of the three solutions, this was considered the one in which the safety of the whole air traffic system was the least certain, but also the least complex and fastest to implement. This solution would also be the back-up solution to the other two.

SOFIA also assumes that TARMS or a similar on-board system is able to provide all the necessary information to the FRF, including up to date databases about the airspace (along with prohibited areas, such as large cities, nuclear reactors, etc.), aircraft status, weather conditions and location of the airports in the area (plus runways and navigation equipment available). If the data link is available these can also be provided from the ground by the GSDS, otherwise the system is dependent on ATIS to confirm the airport conditions. Weather information can also be obtained via the on-board weather radar.

The main goals of the third project, PATIN (Protection of Air Transportation and Infrastructure) [9], were to assess

the key aspects of security in the whole transportation system, as well as to propose an overall warning and information system accessible by emergency response organizations. One of the aircraft in-flight protection systems investigated was passivation. As before, passivation would be monitored by a military interceptor aircraft (mid-term solution) or from the ground (long-term solution). Decisions would be made by the national authorities, connected through an information dissemination system with ATC and military operations centers.

The following functionalities were considered:

- Misuse detection capability through sensors in the passenger cabin and a secure communication path to the ground (as in SAFEE), or through the detection of deviations from the assigned flight path. Unlike SAFEE, decision on whether there is an emergency situation on-board is made by ATM/ATC.

- An ATM/ATC panic button that triggers a holding pattern in order to avoid collision with other aircrafts or with the ground, and to evade a forbidden area. The panic button would also block on-board manual flight controls. This would provide some time to review the situation and all available options. Also considered was an on-board panic button, allowing the pilots or cabin crew to react faster than ATM/ATC.

- Like in SAFEE/SOFIA, an FRF with autonomous flight, sense and avoid, landing and taxiing capabilities. This system calculates a new flight plan considering remaining fuel, weather, airport requirements, etc. These steps would be performed under the supervision of a pilot on ground that can intervene at any time and remotely control the a/c.

PATIN dealt mostly with the need to detect abnormal events taking place inside an aircraft as soon as possible, since in Europe several major airports are located next to cities with important economic and technological centers. Therefore, the concept of a panic button was developed to allow ATM/ATC to confirm the emergency (i.e., to confirm the activation of the passivation system). But unlike in SAFEE, in PATIN the decision center remains on the ground.

In common all three projects acknowledged that modern aircrafts with full fly-by-wire capabilities can already fly an aircraft without human intervention. In fact, they concede that for safety reasons the passivation system needs to be prepared to come up with a flight plan in case communications between the a/c and the ground are affected.

Another important aspect is the need to avoid the inadvertent activation of the FRF. A high rate of false alarms in such a system would be unacceptable for pilots, airlines, air traffic services and the public. Thus the system will have to be made as fail-safe as possible, seeing that it is expected to run without direct human intervention on-board. Finally, it was also recognized that before such a system can be implemented, the acceptance of aircraft crew and the public is required.

As a side note, it should be pointed out that public reaction towards any accident involving new technology, especially if it occurs early in its operation, is likely to be severe [11].

Several technological solutions have been discussed and at this point it is not possible to decide with certainty which will be adopted, if any. But whatever the solution chosen, the passivation system is just one of several new systems under consideration in the growing trend toward increased aircraft automation.

III. COCKPIT AUTOMATION

[12] defined automation as the execution by a machine of a function that was previously carried out by a human. The trend that emerged in the 1970s toward increased automation in the cockpit will continue through the next decades, as new and more powerful computers and technology are developed. One major step in this process was the reduction of the flight crew from 3 to 2, with the elimination of the flight engineer (FE). This was only possible due to the introduction of automated systems that took over most of the tasks traditionally assigned to the FE like, for example, the Full Authority Digital Engine Control, which monitors and has full control of the engines and related subsystems. Another technological enabler was the introduction of the glass cockpit which allowed for the replacement of physical dials and gauges with electronic displays. One of these is the EICAS (or ECAM), a centralized display of system alerts or warnings and engine indications. In recent years, several other systems were introduced with the goal of increasing security, such as the Airborne Collision Avoidance Systems and the Terrain Awareness and Warning System. These warning systems detect traffic and terrain, respectively, in close proximity of the aircraft.

Even more sophisticated is the Flight Management System (FMS), an on-board navigation, performance, and aircraft operations computer. One of its functions is to support automatic flight path control along the lateral, vertical, and longitudinal axes [13]. The FMS has three levels of automation; in the higher level of automation, called the *flight management mode*, the pilot programs a plan into the flight management computer, including route, speeds, and altitudes at different waypoints, and on some aircrafts, arrival time at the waypoints [14]. The pilot's role is to monitor the system and detect any discrepancy and failure. If all goes well, the pilot does not have to touch the controls.

Current Standard Operating Procedures and regulations

in most airlines usually encourage the use of automation during cruise and, under some circumstances, for landing. Consequently, crews no longer fly the aircraft manually, unless they choose to do so. Pilots can usually override the computers, but there are some exceptions. For instance, the introduction of the flight envelope protection means that the pilot is prevented from making control commands that exceed the aircraft's structural and aerodynamic operating limits. In Airbus aircrafts, for example, the pilots can only fly outside the flight envelope by selecting a different "control law", whereas in Boeing aircrafts they are required to use excessive force. In review, airplanes can already fly without any input from the pilots and as technology evolves, they are expected to become more reliable and safe. A passivation system could then be seen as another security layer to the automated systems already in place.

IV. UNMANNED AERIAL SYSTEMS (UAS)

Originally called Unmanned Aerial Vehicles (UAV), Unmanned Aerial Systems consist of the unmanned aircraft and the ground station. Originally UAS were secret military aircrafts developed for reconnaissance and strike in war zones. They now range from small air vehicles that weigh less than 500g to aircrafts weighing over 40 thousand pounds. Today UAS development is undergoing a massive growth associated with the development of new technologies originally introduced to support pilots in the cockpit, like satellite navigation, autopilot, new systems to support navigation, etc. As the costs to build and maintain such systems become smaller, the range of potential civil applications increases: crop surveillance, wildlife monitoring, traffic monitoring, support of search and rescue activities, pollution detection, weather monitoring, airborne crime reconnaissance, etc. [15].

The only thing delaying the civilian applications of UAS are the certification procedures and regulations, including air traffic management procedures, currently under discussion by national and international airworthiness authorities, including the FAA, EUROCONTROL and ICAO. But by 2016 Europe expects to see civil airspace opened to UAS, just one year later than the USA.

One of the proposed civil applications of UAS include cargo transport. In one of the first studies to look at the social acceptance of UAS, [16] reported a survey where 51% of those interviewed were willing to accept cargo transportation by UAS after being provided with detailed information about costs, human error, reliability and availability. In a control group that did not have access to this information only 37% accepted cargo transportation by UAS. When the respondents were asked if they would fly in an unmanned a/c, there were no differences between the two groups in the number of positive answers. However, 35% (vs. 12%) of the "educated" group responded "Not Sure" which suggested that the information provided changed their attitude toward UAS. The author concluded that to increase society's acceptance, UAS information should be slowly provided to the public. Finally, another interesting finding was that only around 12% and 17%, respectively, of the respondents said they would fly in an unmanned a/c if prices were 50% cheaper.

Familiarity brings acceptance, and as people become more familiar with UAS, they will be more willing to accept them. As reported by [16], there is already some support to the use of UAS for cargo transportation. Once it becomes a reality, trust in the technology behind the system should increase and, once the risks are deemed small enough, society might be more willing to accept the transport of passengers by UAS. It is reasonable to assume, though, that passenger transportation by UAS is even more remote in time than aircraft passivation. A more realistic approach is that social acceptance of cargo transportation by UAS could pave the way for a system like aircraft passivation in commercial airlines which, in turn, could lead to a greater acceptance of UAS transporting passengers in the long-term.

V. LESSONS LEARNED BY THE AUTOMOTIVE INDUSTRY

Driverless cars are no longer a thing of the future. Currently several car companies are testing the prototypes of cars that do not require human intervention and it is expected that before 2025 they will be ready for the market [17]. Two of the arguments for the introduction of driverless cars is that it maximizes road capacity and reduces driver error [18]. [19], for example, reported that approximately 90% of all traffic accidents are caused by human error due to fatigue or inattention. Therefore, some argue that computers are actually safer than humans considering that they do not run red lights and do not go over speed limits, for example.

A survey of 407 drivers from 9 European countries conducted in SAVE [20], a EU project aimed to develop a system that takes over vehicle control in case of an emergency, showed that handing control to a device was evaluated as a negative aspect of such a system. Drivers expressed concern over "loss of control" and were only willing to hand over control in emergency situations, such as driver breakdown [20]. In a different study, [21] tested drivers' acceptance of an Adaptive Cruise Control system and found an almost unanimous objection to automatic braking, because it "crossed the red line that dictates who controls the vehicle". What the automobile industry has discovered is that systems that take over control are usually disliked by the public [22].

In CVIS [23], an FP6 EU project which evaluated intelligent transport systems for road transport, a survey assessed how acceptability changed if the public had to pay for these new systems. The authors found that the percentage of acceptance of new car technology

decreases on average 25% when the drivers are asked about the willingness to pay for it [23]. Furthermore, the authors concluded that in order for society to accept these advanced technologies, they should be introduced concurrently with actions to encourage adoption and acceptance. These include, among others, emphasizing safety, economic growth and job generation.

VI. THE ISSUE OF SOCIAL ACCEPTANCE

The overall acceptability of a computer system can be measured in terms of social acceptance and user acceptance [24]. The former is determined by society's perception of the benefits vs. the risks or drawbacks of adopting such a system. The latter includes the evaluation of the ergonomics of the system, considering features such as cost, reliability, usability, compatibility with other systems, etc. [22]. A system can have high scores on user acceptance, but low on social acceptance and, thus, be rejected. Some aspects to consider are the moral issues involved and the social, political, economic, and institutional environments surrounding the technology [11, 25].

Technology seems to have reached a point where the most important question is not "can we do it?", but "should we do it?". And the public wants to have a say in the matter. With a few exceptions, nowadays people are less inclined than a few decades ago to enthusiastically and uncritically accept technology, even if it has a strong support from the government and scientists. The nuclear accidents in Chernobyl and Fukushima, the destruction of the ozone layer by the chlorofluorocarbons (CFCs) used in sprays and infant malformations caused by the drug Thalidomide, are reminders that sometimes innovation can go terribly wrong. Events like these also affect the level of trust that society has on its scientists and engineers. If science is considered objective, people will be more willing to accept the professional opinion of researchers. However, if science is seen as vulnerable to bias and prejudice, society will reject its conclusions [25], and thus dismiss scientists' assurances that a system is safe.

Several researchers consider that the most influential cultural dimension in determining technology acceptance and usage is Uncertainty Avoidance, or UA [26, 27]. As the name suggests, UA is a measure of society's tolerance for uncertainty and ambiguity. The higher the UA scores, the greater the resistance to change. Resisting change, however, is not the same as resisting technology. In fact, high UA societies are more likely to embrace technology as a means to reduce unstructured and unpredictable situations. The adoption will not occur immediately, though, as these countries will usually observe the experiences of other countries before adopting the technologies themselves. Low UA countries, on the other hand, tend to value innovation, risk and accept innovations more easily [27]. Japan, France and Germany are examples of countries with high UA scores, whether the US, the UK and Denmark are among the countries with the lowest UA scores in the World.

Nevertheless, even the data on uncertainty avoidance are not enough to allow us to make clear predictions regarding acceptability of new technologies. For example, unlike Germany and Italy, France's nuclear power program was accepted without much opposition [28] and all three countries have relatively high UA scores (especially France and Italy). More relevant seems to be the perceived transparency and degree of confidence in the decision-making process. In other words, the political and institutional specificities of each country explain people's behavior toward new technology better than the countries' UA score. As reported by [29], the public focuses on three main aspects when deciding if a new technology is acceptable:

- Is the decision-making process about the technology acceptable to those who would suffer the consequences of an accident?
- In case of an accident, is the process to decide responsibility and accountability accepted by those affected?
- Do people trust those making the decisions?

French society, for example, is in general more supportive of the decisions made by the state and public administration than the Italian and American societies [28], which suggests that there might be less opposition against a passivation system in France than in Italy or the USA.

Also important is the perceived risk associated with the technology, that is, the risk as judged intuitively by the public as opposed to that measured by the experts, which in most cases do not match. Risk perception is influenced by several related factors. For [28] the most important are the perceived benefits for the individual (the greater the benefits, the smaller the perceived risk) and the global feeling of security provided by society, which depends on the socioeconomic status, as well as on physical and mental health. For example, low income and lack of social relationships are associated with overestimation of risks.

Another important characteristic of risk perception is that accident magnitude is usually given more weight than probability of occurrence [29]. For example, in the eyes of the public, a failure in the technology that causes 300 deaths is unacceptable even if it occurs only once in 10 000 years, whereas for an expert this fatality rate might be acceptable considering the benefits.

Also, when society has no control over the outcome once in the risk situation, the less the level of risk it is willing to accept [29]. For example, people are more willing to accept the risks associated with skiing than with flying

since they have much more control over the situation and are not dependent on the skill of others. Society also expects a higher level of protection from involuntary than from voluntary risks (e.g., the presence of a nuclear power plant in the area vs. riding a motorcycle) [11]. Finally, if the technology forces dependence upon small groups of technical elites, if it requires strict physical security measures or special police powers, or if it increases the power of big business, society will develop a negative perception of it [11].

A. Social acceptance of the passivation of misused aircraft

Assuming the passivation system is deemed to be safe and reliable by the regulation authorities, the stakeholders of the aviation industry will have a very important saying regarding its introduction in aircrafts. For aircraft manufacturers and airlines, a very important issue would be the costs associated with introducing the system in new aircrafts. Retrofitting of current aircrafts would probably not be economically viable given the technical complexity of the upgrades [7]. If it becomes more expensive to buy and maintain aircrafts, the airlines will attempt to cover the costs by increasing ticket prices. And, as with the driverless cars, passengers might not be willing to pay for it even if a strong case is made of increased safety, because aircrafts are already perceived as being quite safe. A more realistic possibility is that the new system would be introduced in a whole new generation of aircrafts.

The situation for the pilots is of another nature and one might expect the biggest opposition to come from them since they would be directly affected by the system. In the current environment, any system that reduces the pilot's authority in the cockpit will probably be met with some resistance. Here the major question is: Will the pilots accept a system that, under some conditions, might take control of the aircraft from them? Recall that the activation of the passivation system in an aircraft will ultimately be dependent on the pilots' behavior. If their behavior is erratic or raises red flags, the system might be activated. Therefore, several aspects will need to be clarified, including the Standard Operation Procedures and the system's engagement and disengagement conditions, an issue also raised by the pilots surveyed in SAFEE. If someone threatens to break into the cockpit, should the system be immediately activated (as a deterrent to further actions)?

Finally, pilots might also oppose such a system if they see it as one more step toward full cockpit automation and, thus, job loss. In a shorter-term there is some risk that regulations on working hours and rest periods could be loosened up. If a new safety layer is introduced, such that an a/c can land even if the pilots are incapacitated, airlines will most likely pressure the authorities to allow such a reduction.

In terms of public acceptance of passivation, one very important aspect is the need to introduce some mechanisms which define the conditions under which national authorities can passivate an aircraft, especially one from a different country flying over its territory. As discussed earlier, current ICAO conventions state that the responsibility for dealing with security incidents remains with the states that are dealing with the emergency. In theory, however, what would prevent a country from activating the passivation system of an a/c if authorities suspect that a fugitive is on-board?

The benefits of passivation should also be made clear, as they will greatly influence the public's willingness to accept the risks. Passivation needs to be presented as a countermeasure to terrorist actions that improves safety. And society might need to be reminded that currently there are only two approaches to deal with a hijacked aircraft: escorting it by fighters in order to force it to land, or destroying it in case a catastrophic event needs to be prevented [9]. Even dispatching military jets to meet the suspicious a/c can take several precious minutes as the time from flight path deviation to impact can be shorter than the start-up time for the fighter. Additionally, as already mentioned, one needs to consider the damage that the debris resulting from shooting down an a/c might have on the people and structures on the ground.

Earlier in the paper it was pointed out that the type of technology would also influence the degree of public acceptance. As seen in SAFEE/SOFIA and PATIN, there are two different decision-making procedures that need to be allocated. The first one is whether the decision to passivate an a/c remains in the a/c or on the ground. The second is where the flight plan is generated. To leave both decisions to aircraft systems means humans would be giving up control, which might lead to a greater resistance to their acceptance by the public. I suggest that we avoid the temptation to automatize the decision-making process and that humans should be kept involved whenever possible. In other words, total automation of the passivation system should be seen as a back-up plan when all else fails: it should not be the only solution.

In review:

- System should be safe and reliable with a low rate of false-alarms.
- Solicit and incorporate feedback from pilots.
- Decision-making process should be clear and transparent (who passivates and under which conditions).
- The more familiar people are with the technology, the easier it will be to accept it.
- Promote the benefits, point out the alternatives.
- Stress that the passivation system is to be used only

in emergency situations when the pilots are incapable of flying the a/c.

REFERENCES

[1] ICAO, 2013 Safety Report, 2013.

[2] M. Grabell, "History of the federal air marshal service", Retrieved from http://www.propublica.org/article/history-of-the-federal-air-marshal-service, 2008.

[3] M. Tresselt, "Renegade flights and the tragic choice: must the State sacrifice innocent people?," Paper presented in the Workshop of the 5th Berlin Roundtables on Transnationality, Retrieved from http://www.irmgard-coninx-stiftung.de/fileadmin/user_upload/pdf/ archive/Matthias_Tresselt_III.pdf, 2006.

[4] European Cockpit Association, Pilot Fatigue. Brussels, Belgium: ECA, 2012.

[5] ICAO, Fifth meeting of the ALLPIRG/Advisory Group (ALLPIRG/5-IP/7), 2006.

[6] EUROCONTROL, Annual Report 2005, 2006.

[7] SAFEE Consortium, SAFEE (Security of Aircraft in the Future European Environment), Final Publishable Report (EC contract number AIP3-CT-2003-503521), 2008.

[8] SOFIA Consortium, SOFIA Final Publishable Activity Report (EC contract number AST5-CT-2006-030911), 2010.

[9] D.-R. Schmitt, H. Többen, and H. Philippens, "Passivation of Misused Aircraft to Protect Passengers, Airports and Infrastructure," Proc. 27th ICAS, 2010.

[10] O. Laviv, and L.J.P. Speijker, SAFEE - Security of Aircraft in the Future European Environment (Report no. NLR-TP-2006-716). Amsterdam, The Netherlands: NLR, 2007.

[11] R.A. Clothier and R.A. Walker, "Determination and Evaluation of UAV Safety Objectives," In Proc. of the 21st Int. Unmanned Air Vehicle Systems Conf., pp. 18.1-18.16, 2006.

[12] R. Parasuraman, and V. Riley, "Humans and automation: Use, misuse, disuse, abuse", Hum Factors, vol. 39(2), pp. 230–253, 1997.

[13] C. D. Wickens, "Aviation Displays," in Principles and practice of aviation psychology, P.S. Tsang and M.A. Vidulich, Eds. Mahwah, NJ: Erlbaum, 2003, pp. 147-200.

[14] S. Dekker, and E. Hollnagel, Coping with computers in the cockpit. Aldershot, UK: Ashgate, 1999.

[15] FAA, Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap. Washington, DC: US Department of Transportation, 2013.

[16] S.L. MacSween-George, "Will the public accept UAVs for cargo and passenger transportation?", Proc. Aerosp. Conf. , vol. 1, pp. 1-11, 2003.

[17] C. Wüst, "Auto Revolution: A Promising Future for Self-Driving Cars," Spiegel Online International, February 2013.

[18] D. de Waard, M. van der Hulst, M. Hoedemaeker, and K.A. Brookhuis, "Driver behavior in an emergency situation in the Automated Highway System," Transp. Hum Factors, vol. 1, pp. 67-82, 1999.

[19] K.A. Brookhuis, D. de Waard, and W.H. Janssen, "Behavioural impacts of advanced driver assistance systems–an overview," EJTIR, vol. 1, pp. 245-253, 2001.

[20] S. Petica, and E. Bekiaris, Driver needs and public acceptance of emergency control aids. SAVE (TR1047) EU Project Deliverable 3.1. Arcueil, France: INRETS-DERA, 1996.

[21] M. Hoedemaeker, and K.A. Brookhuis, "Behavioural adaptation to driving with an adaptive cruise control (ACC)," Transport Res F-Traf, vol. 1, pp. 95-106, 1998.

[22] J.D. van der Laan, A. Heino, and D. de Waard, "A simple procedure for the assessment of acceptance of advanced transport telematics," Transport Res C-Emer, vol. 5, pp. 1-10, 1997.

[23] J. Pauwelussen, M. Hoedemaeker, and L. Kistemaker, Utility, Usability and User Acceptance requirements (D.DEPN.4.1), CVIS Project, 2010.

[24] J. Nielsen, Usability Engineering, San Diego, CA: Academic Press/Morgan Kaufman, 1993

[25] R. Pool, Beyond Engineering: How Society Shapes Technology: How Society Shapes Technology, Oxford University Press, 1997.

[26] P.W. Cardon, and B.A. Marshall, "National culture and technology acceptance: The impact of uncertainty avoidance", Issues in Inf Syst, vol. 9, pp. 103-110, 2008.

[27] T. Vörös, and J. Choudrie, "Uncertainty Avoidance and Technology Acceptance in Emerging Economies: A Comparative Study," SIG Globdev 4th Ann Conf, Shanghai, China, 2011.

[28] S. Bastide, J.P. Moatti, and F. Fagnani, "Risk perception and social acceptability of technologies: the French case," Risk Analysis, vol. 9, pp. 215-223, 1989.

[29] S. Rayner, and R. Cantor, "How Fair Is Safe Enough? The Cultural Approach to Societal Technology Choice1," Risk Analysis, vol. 7, pp. 3-9, 1987.

[30] H. Otway, and D. Winterfeldt, "Beyond Acceptable Risk: On the Social Acceptability of Technologies," Policy Sciences, vol. 14, pp. 247-256, 1982.

EMAIL ADDRESSES

ana.martins@dlr.de

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

Section 2. Architecture and Solution Definition

This section of the book describes the process by which concepts and requirements are translated into a detailed architectural framework.

The development of a new architecture for the future European ATM security requires a clearly defined methodology in order to enhance the productivity, taking into account the constraints inherent in complex systems like the European ATM.

The first article of this section looks into the methodology applied to develop the GAMMA architecture. The article provides some background into the need for a common frameworks and language and the importance of modelling.

The choice of framework and tool used in GAMMA for architectural modelling was based on the wish to maintain compliance with the approach taken in SESAR, which adopted the NAF V3.1 architecture framework and the Mega tool. The article therefore describes the process of tailoring NAF for the GAMMA context and the main steps of the architecture development methodology applied. Emphasis is given to the way the methodology is focussed to overcome the challenges inherent with international geo distributed teams, each coming with different competencies and experiences.

The advantages of adopting an architecture development methodology based on a standard framework and language are highlighted within the context of GAMMA, serving as an important lesson for future initiatives.

The second article in this section takes a much higher level view on how the concept outlined in section 1 is instantiated in practice through concrete technical developments. This vision for the enhancement of ATM security in Europe is realized, within the GAMMA project, by the development of a central prototype named Security Management Platform (SMP), specifically developed to recreate the GAMMA concept, and additional prototypes that support the proposed concept. Security related information is sent to the SMP by six peripheral prototypes, representing specific security enhancements applied to the ATM domain (cyber security, CNS etc).

The 7 prototypes developed within GAMMA are intended as a small scale reproduction of the GAMMA architecture. These prototypes should therefore be seen as a selection from a far wider set of functionalities and security enhancements envisaged within the full architecture.

***Lalitha Abhaya**, Airbus Defence and Space*

GAMMA Architecture Development methodology

Lalitha Abhaya, *AIRBUS DS SAS*

The GAMMA ATM Security proposed solution is intended as a contribution to resolve the security issues and gaps identified within ATM. While the enhancements in ATM architecture are defined within the SESAR project, the aim of the GAMMA project is to demonstrate the feasibility of security improvements within the ATM system of systems. The development of a new architecture for future European ATM security requires a clearly defined methodology in order to enhance the productivity taking into account the constraints inherent in complex systems like the European ATM.

Prior to describe the methodology applied to develop the GAMMA architecture, the importance of defining architecture and a methodology is briefly discussed within this introductory section.

Challenges of System of Systems evolutions

The complexity of Systems of Systems (SoS) such as ATM increases the challenges for stakeholders creating solutions to improve the functionalities of the whole system or any individual system constituting the SoS. Furthermore, the engineering teams are distributed in time and space and composed of many companies, each with their own culture, methods and tools. The purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related and consistent with each other.

Architecture description and need for frameworks and common languages

The conceptualization of a system's architecture, as expressed in an architecture description, assists the understanding of the system's fundamental nature and key properties pertaining to its behaviour, composition and evolution, which in turn affect concerns such as the feasibility, utility and maintainability of the system.

Architecture frameworks and architecture description languages are being created as assets that codify the conventions and common practices of architecting and the description of architectures within different communities and domains of application. An architecture framework contains standardized views, sub-views, templates and guidelines, meta-models, etc. that facilitate the development of the views of a system architecture. A view addresses a particular stakeholder concern (or set of closely related concerns) and specifies the kinds of models to be used in developing the system architecture to address that concern.

Importance of the modelling

A model is a simplified representation of a system at some particular point in time or space intended to promote understanding of the real system. As an abstraction of a system, it offers insight into one or more of the system's aspects, such as its function, structure, properties, performance, behaviour, or cost.

The use of modelling during the early stages of the system design serves to make concepts concrete and formal, enhance quality, productivity, documentation, and innovation, as well as to reduce the cost and risk of systems development. Clear definition of the architecture using appropriate models helps to highlight any inconsistencies or problems early in the project lifecycle to be better communicated and easily understood by the stakeholders. This enables the team to work in an integrated coherent fashion by improving the team's ability to collect, analyse, improve, share and manage the architecture data.

Methodology

A methodology describes how to realise commonly known system design processes using the most suitable framework, modelling language and a tool for the project of interest. The choice for the framework and tool to be used is implicit in order to be consistent with SESAR project which is using the NAF V3.1 architecture framework, and the Mega tool.

The major steps of the architecture development methodology used in GAMMA are briefly described in the following sections.

Tailoring NAF

The NAF is tailored according to the well experienced approach MMP (modelling Management Process) applied within most of Airbus projects. The architecture objectives are defined at the beginning of this approach in order to establish the project specific meta-model. The meta-model of the project defines a common vocabulary and the concepts as well as the relationships between them. These are the concepts which are instantiated within architectural views during modelling. The

coverage of the project's Meta -model concepts by NAF Meta-model concepts are realised as each NAF view includes a particular set of NMM (NATO Architecture Framework Meta Model) concepts. For example a NOV (NAF Operational View), mainly includes Operational Nodes and describes Operational Activities, including Information elements exchanged between Operational Activities and Nodes. This activity leads to identify the architectural views to be produced and results in a tailoring of the NAF views as NAF 3.1 defines more than 40 sub views. The selected NAF views are the ones which are the most suitable to respond to the architecture objectives. The final step is to map the concepts used in NAF views to the objects of the meta model specific to the tool used, in this case Mega suite. The modelling rules and guidelines are derived from this mapping.

Define the architecture development method

Once the modelling approach is specified, the activities of the architecture development and associated outcomes are defined in accordance with the availability of inputs from other GAMMA work packages. Focus is given to enhance the productivity of the geo distributed architecture team. Moreover, the content inputs are provided under different formats (Excel tables, Power Point diagrams etc.) by the team members to the architecture repository responsible. The main activities of this method and the NAF views produced are described below:

- Model Threat scenarios (NSV-6c): Clarifies the impact of threat scenarios on supporting assets which should be protected by putting in place the security solution. The activity helps to ensure that the architecture solution actually covers the considered threats.

- Define the operational nodes and processes taking as input the Security controls previously defined within the project (NOV-2, NOV-5)

- Produce the hierarchical breakdown of the operational processes (NOV-5)

- Define system architecture elements (Security Control Assets) based on the security controls

- Define security systems/sub systems, their functions and the interactions between them (NSV-1, NSV-4)

- Produce system views: helps to describe how the sub systems interact and how they interface with ATM architecture

- Produce high level pictures of the operational architecture and system architecture (NOV-1)

- Establish mappings between architecture views and produce consistency reports

This method is depicted in the following figure.

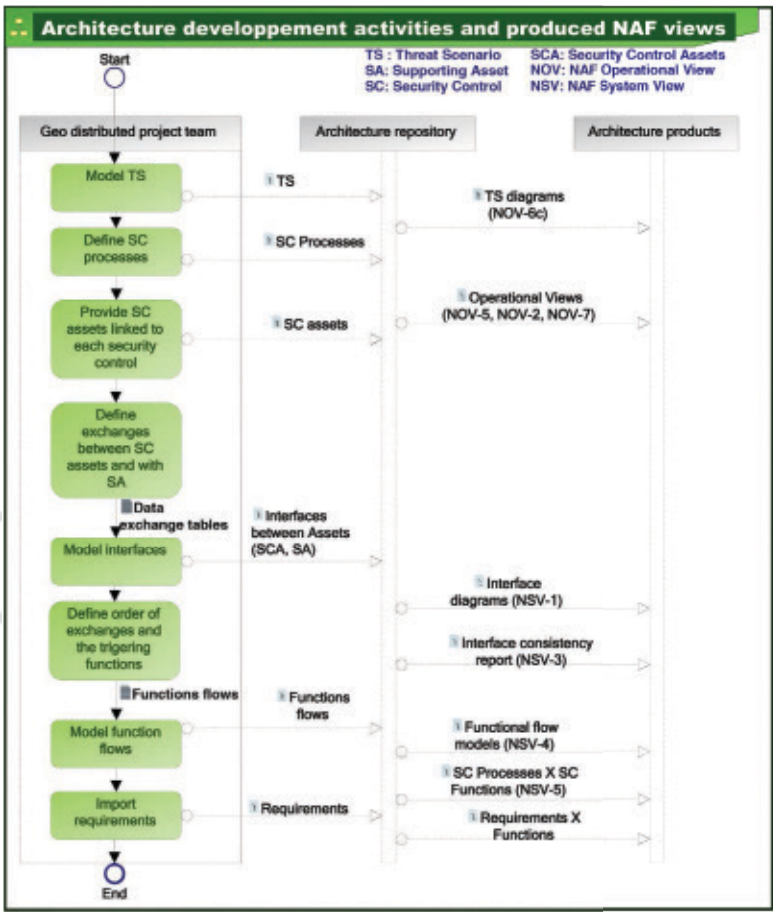


Figure 1: Architecture development activities and outcomes

In addition to the above mentioned views, many other views are produced to check the consistency, and the traceability of the architecture. These views include:

- NSV-3: System-System Matrix presenting the summary of interfaces which help to check the interface consistency

- NSV-5: System Function to Operational Activity Traceability Matrix

- NOV-7: High level model of the information exchanged between ATM nodes

Setting up the repository and the document templates

This activity consists of configuring the architecture repository for easy search and queries, consistency analysis, and document generations. To facilitate search and queries the objects used in models are tagged with appropriate keywords. In order to generate the deliverable document from the contents of the repository, templates are configured.

Producing the templates to input architectural data

As mentioned earlier the GAMMA architecture team is geographically distributed and the selected tool competency is centred within Airbus. So it is very important to define the templates and guidelines in order for the team to contribute efficiently to the modelling of the architecture. These templates are proposed mainly in tabular form, but some are defined in the form of Visio or PowerPoint diagrams according to the preference and the convenience of the input provider.

Establishing model review checklists

As the cross check reviews are made to ensure the models quality, the check lists are produced to help this activity, specially the syntax of the models. Considering the content checking, the expert knowledge can't be replaced by a check list, but some points are also included in the check lists to support the quality checking.

Producing models and consistency reports

Based on different content inputs in tabular form or as diagrams, the models are established within the architecture repository. Several consistency reports are configured at the beginning of the modelling to check the consistency as the modelling progresses. Once the models are produced within the repository they are exported again in the required formats as diagram or tables in order to be reviewed and discussed by the team.

Generate models and deliverable documents

Deliverables and some tabular reports are generated automatically at the end of the architecture definition process. The major advantage of this functionality is to avoid the inconsistencies which happen frequently within the process of writing a document by more than one person.

The document can be generated each time the updates are made to the architecture. All the post review updates are also entered into the repository and then the final deliverable is generated which contains the latest information.

Conclusion

The architecture development method and the modelling approach defined at the beginning of the architecture definition activities contributed largely to the success of the GAMMA Architecture and the teamwork. It helped to overcome the many challenges inherent with international geo distributed teams coming with different competencies and experiences. In addition, the architecture artefacts produced according to the methodology contributed to improve the productivity of system engineering activities, such as integration and validation. This highlighted again within the context of GAMMA, as it had within SESAR, the advantages of adopting an architecture development methodology based on standard framework and languages.

The GAMMA concept and its technical instantiation

***Claudio Porretti**, Leonardo*

The **Global ATM Security Management** (GAMMA) proposed solution builds on the principles and concepts related to Security Management in a collaborative multi stakeholder environment, while maintaining a strong link to the current international and European legal framework and the constraints given by the respect of national sovereignty.

The GAMMA architectural vision remains therefore rooted in the fundamental principle that Security is a national responsibility which cannot be delegated, while recognizing the opportunity opened up by a collaborative framework for managing security.

This vision for the enhancement of ATM security in Europe is instantiated, within the GAMMA project, by the development of a central prototype named **Security Management Platform (SMP)**, specifically created to realize the GAMMA concept, and additional prototypes that support the proposed concept.

The SMP will be the core component of the GAMMA technical solution and provides an information sharing platform collecting and processing security information as well as distributing it on a strict rule based principle. Security related information is sent to the SMP by six peripheral prototypes, representing the specific security enhancements applied to the ATM domain (cybersecurity, CNS etc).

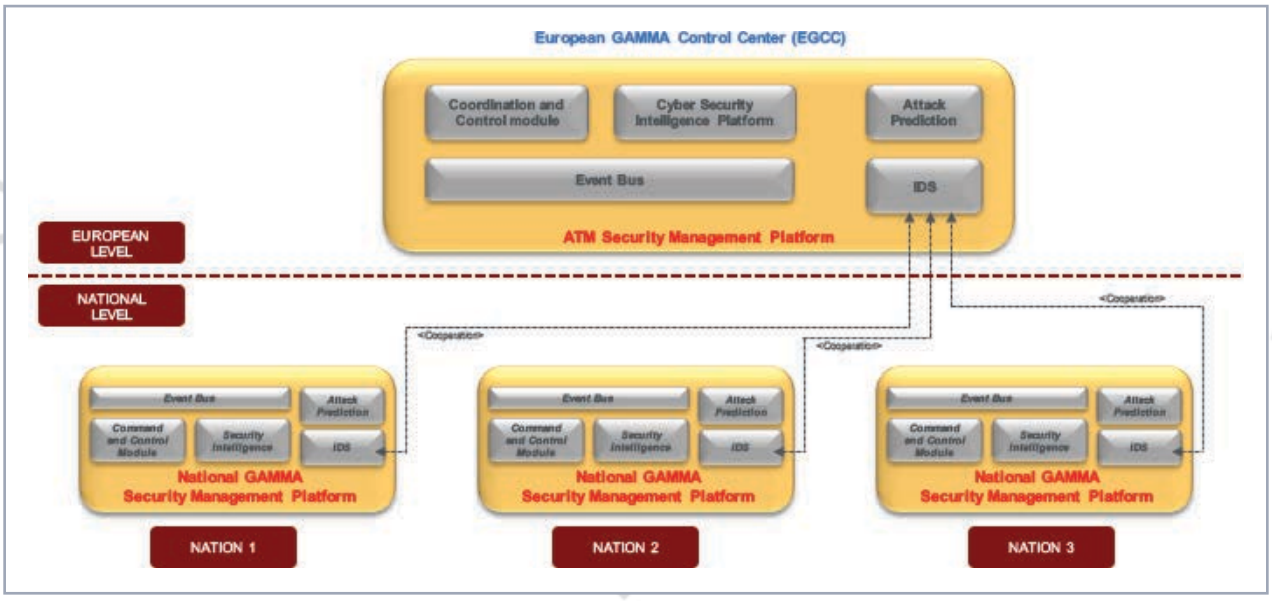
The SMP is intended to provide improved situational awareness and decision support functionalities supporting the coordinated management of ATM security. For this purpose the shared platform includes specific capabilities such as **Cyber Security Intelligence** and **Attack Effect Prediction**, in order to provide decision support to GAMMA operators. Moreover, the SMP includes an **Information Dissemination System** that allows the dissemination of security information through the multilevel architecture proposed by the GAMMA technical solution.

Multilevel approach

The GAMMA concept can be illustrated as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.

GAMMA defines three different layers for managing Security:

- **Local level**, (represented either by a local security system or a Local GAMMA Security Operation Center, **LGSOC**),
- **National level**, (represented by the National GAMMA Security Management Platform, **NGSMP**)
- **European level** (represented as European GAMMA



Multilevel approach

Coordination Centre-**EGCC**).

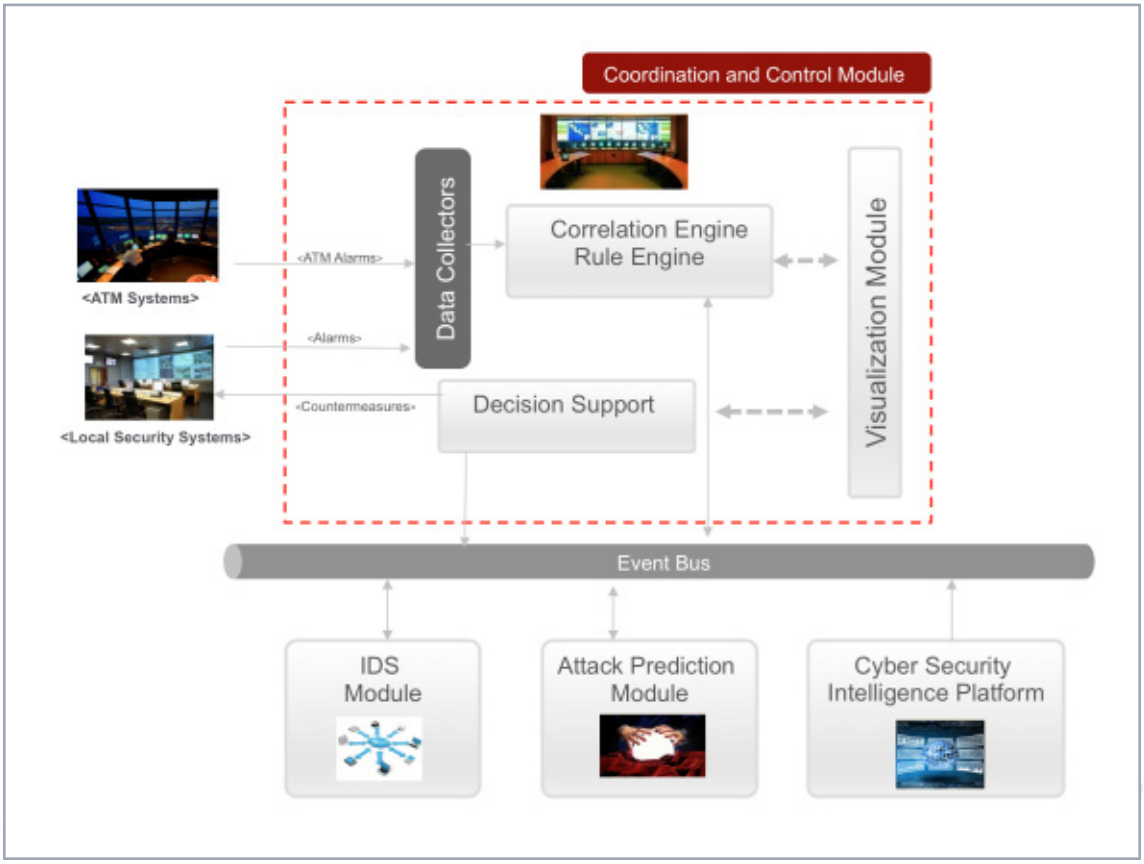
In terms of instantiations of the SMP this kind of approach implies:

- one SMP instance in the EGCC
- one SMP instance for each NGSMP

SMP main functions

- **Command & Control System**: Provides Alarm Correlation, Security Monitoring and Decision Support for Incident/Crisis Management
- **Attack Effect Prediction**: Provides prediction for the adversary actions and possible (expected) impact based on the information received from the SMP.
- **Cyber Security Intelligence Platform**: provide information regarding emerging threats to ATM security, Social and Political contingencies with a possible impact on ATM security.
- **Information Dissemination System (IDS)**: provides automatic dissemination of security reports from the SMP at European level to connected SMPs at National levels, applying filtering conditions, and allows the SMP operator at National level to disseminate manually security reports to other connected Security Management Platforms at national or European level.

The following figure represents the high level architectural layout of the Security Management Platform:



SMP architectural lay-out

SMP proactive capabilities

- Through the Cyber Intelligence Module the operator can find information affecting the security of the air traffic domain. Such information can be disseminated to instances of the SMP in other countries as well as to the SMP in the EGCC for European coordination
- Through the Attack Effect Prediction module (AEPM), the GAMMA operators can obtain a prediction for the adversary actions and possible (expected) impacts based on the information received from event detectors. The AEPM estimates the possible strategies which are most probable, listing possible counteractions, given the estimated attacker strategy and event detectors values
- Through the Decision Support module, the GAMMA operator can obtain a list of possible countermeasures (that have been recorded earlier) in relation to alarms received from ATM connected systems and Local Security systems

SMP modules

The high-level architectural view of the Security Management Platform is elaborated below. It is composed of the following software modules:

• **Data Collector Event bus**: this module includes different filters that collect and normalize event data stream coming from different ATM systems. It is the enterprise application bus that enables the cooperation among different modules.

• **Coordination and control**: this function is subdivided in the following modules:

- **Correlation Engine**: this module is composed by a framework that allows stream event processing. Each stream will be produced by elements located in the ATM domains and sent to the "Data Collection" modules. After the normalization tasks, they will be forwarded to the Correlation Engine for elaboration and correlation activities.

- **Rule Engine**: this module is used to configure the correlation policies (Signature Based or Anomaly Based) that will be applied to the stream by the Correlation Engine.

- **Decision support system**, The Decision Support system gives support to GAMMA operators in case of an attack, providing possible countermeasures; such countermeasures are stored in a database fed with information coming from Cyber Security Intelligence module and attack effect prediction module

• **Visualization Module**: this module is used to visualize the correlated information using different real time and batch views. In this module IDS offers a visualization of the received events in real-time and fuses the received ATM data (like track, plot, and basic flight plan information) from the ATM systems and the received events from the Event Bus into one reliable, comprehensible overview.

• **Cyber security Intelligence Platform**: it is the Cyber Intelligence web portal through which it is possible to view the Intelligence bulletin or advisory alerts. The module is connected to an external service that crawls and mines specific external public sources (i.e. social networks, etc) in order to find relevant information for ATM security and ATM threat prevention.

• **Attack Effects Prediction module**: this module is intended to predict possible actions of the attacker and use it to predict the impact. The impact prediction comes as a consequence of the prognosis of possible threats. This module will perform a ranking of possible threats based on sensor values and disseminate that ranking.

• **Information Dissemination System (IDS)**: IDS provides an awareness of all security alerts of all connected systems to the SMP. IDS presents the reported security alerts of the connected system under attack in both the temporal and positional domains on a concise situational awareness display with the possibility to zoom to the infrastructure level or system level (when the infrastructure and systems are stored as maps in IDS). IDS disseminates security information manually and automatically (e.g. alarms, security information, intelligence information) to other connected Security Management Platforms at national or European level. Filtering algorithms or manual actions apply restrictions to the dissemination of security information based on the sensitivity of the information and on other attributes.

Section 3. GAMMA Security Functionalities and Prototypes

In the GAMMA project, a set of prototypes have been developed and then integrated with a validation environment to demonstrate the concepts elaborated in the project and described in the first section of this publication.

The GAMMA concept has been realized in experimental environments through 7 prototypes. The Security Management Platform prototype, or SMP, represents the core of the concept, implementing the principles of cooperative management of ATM security outlined in the vision. It is based on an information sharing platform for improved situational awareness and decision support functionalities.

The SMP is fed by security related information sent by the other 6 prototypes acting as alert detectors, each representing specific security enhancements applied to the ATM domain and providing defense against security attacks at local level. All prototypes are therefore able to communicate with the Security Management Platform prototype, which lies at the heart of the GAMMA Security architecture. The articles in this section cover all the prototypes developed in the project:

1) Security Management Platform (SMP)
2) Secure ATC communication (SACOM)
3) Information Security System (ISS)
4) Integrated Modular Communication (IMC)
5) SATCOM Security
6) Secure GNSS Communication
7) Information Exchange Gateway (IEG)

This section also includes articles on two important modules of the Security Management Platform: Information Dissemination system (IDS) and Attack effect Prediction modules

The IDS functionality implements the principle of controlled distribution of information which lies at the heart of the GAMMA proposed solution. The Attack Effect Prediction (AEP) Module is a decision support sub-system that provides a joint assessment of the information received from different sensors (event detectors) represented in the system, providing an estimation of the expected impact based on predefined impact values, estimated adversary's skills and implemented security controls' properties.

The 7 prototypes developed in GAMMA are intended to recreate in a small scale the vision outlined in the concept so as to provide a platform for its validation. The validation activities are described in detail in section 4 of this book.

Claudio Porretti, *Leonardo SpA*

A New Vision for ATM Security Management

The Security Management Platform

***Claudio Porretti**, Security and Information Systems, FINMECCANICA S.p.A. (Rome, Italy)*
***Denis Kolev**, University of Lancaster (Lancaster, UK)*
***Raoul Lahaije**, 42Solutions (Eindhoven, The Netherlands)*

ABSTRACT

The aim of this paper is to describe a new vision for ATM Security Management that is proposed by the GAMMA project, and implemented by its "core" prototype called ***Security Management Platform***.

GAMMA is an FP7 project with the goal of developing solutions capable to manage emerging ATM vulnerabilities. The GAMMA vision recognises the opportunities opened by a collaborative framework for managing security, building a solution based on the self-protection and resilience of the ATM system, with the possibility to share security information in a distributed federated environment.

This concept is implemented with the Security Management Platform prototype, and can be conceptualized as a network of distributed nodes embedded within the ATM system, providing interfaces to (ATM) internal and external security stakeholders.

The Security Management Platform prototype provides a basis for the management of security throughout phases, from prevention to the identification of security incidents and the efficient resolution of the resulting ATM crises.

Keywords: ATM, Security Management, Vulnerabilities, Collaborative Framework, Security Information Sharing.

I. INTRODUCTION

The GAMMA vision is to adopt a holistic approach for assessing ATM security, maintaining alignment with SESAR and reaching the following main objectives:

- Extend the scope of threat assessment performed within SESAR to a more comprehensive system of systems level, inclusive of all ATM assets and all forms of threats.
- Develop a Global ATM Security Management framework, representing a concrete proposal for the day-to-day operation of ATM Security and the management of crises at European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.
- Design and implement prototype components of the GAMMA solution so as to demonstrate the functionalities and operations proposed for the future European ATM.
- Set up a realistic validation environment, representative of the target ATM solution, through which to perform validation exercises aimed at validating the feasibility and assessing the adequateness of the procedures, technologies, and human resources issues proposed.

II. THE CONTEXT

The new ATM system must take into account the changes in security risk profiles, due to cyber attacks, telecommunication systems spoofing and ground physical attacks, that according to the new ATM architecture can spread their negative effects from one node to a global level, due to chain reactions and domino effects.

This situation calls for a holistic vision of ATM security, as pursued by GAMMA, to ensure:

- Continuous sharing of security information among the different ATM actors, providing overall situational awareness of the security status of the ATM as a whole, as well as a basis for identifying threats through extended correlations of isolated incidents;
- Means for supporting the resolution of the security crises, minimizing disruptions and repercussions to the system as a whole
- Improved capabilities (operational and technological) to face emerging threats.

III. THE CONCEPT OF OPERATIONS

The GAMMA Concept has been defined having in mind principles and concepts related to Security Management in a collaborative multi stakeholder environment

The GAMMA solution can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.

GAMMA establishes three different levels for managing security:

- the European level represented by the European GAMMA Coordination Centre (EGCC),
- the National level represented by the National GAMMA Security Management Platform (NGSMP)
- the Local level represented by local security systems as well as Local GAMMA Security Operation Centers (LGSOC).

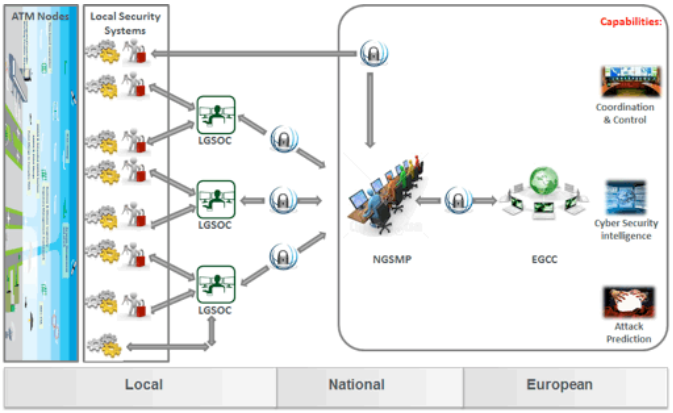


Figure 1: The GAMMA Concept.

The most important concept of the GAMMA project is the sharing of security information such as security alerts, possible countermeasures, security reports, between ATM stakeholders.

The sensitive information, generated at local and national level, that has to be disseminated to the European level, can be (if necessary) opportunely modified so as to eliminate sensitive aspects.

IV. THE SECURITY MANAGEMENT PLATFORM

The federated architecture concept mentioned above is implemented by the Security Management Platform (SMP) prototype.

The SMP is intended to provide Situational Awareness (applying cross-correlation techniques of events) and Decision Support functionalities, supporting the coordinated management of ATM security.

For this purpose the shared platform includes specific capabilities such as Cyber Security Intelligence and Attack Effect Prediction, in order to provide decision support to GAMMA operators, that are the stakeholders interfacing the SMP system, with the aim of managing ATM security.

Moreover, the SMP includes an Information Dissemination System that allows the dissemination of security information through the multilevel architecture proposed by the GAMMA solution.

A. Architecture

The SMP subsystems are connected through an enterprise application bus (Internal Event Bus) that enables the cooperation among different modules.

Another application bus (External Event Bus) is used to connect the national level SMP to the European level SMP and to local security systems such as LGSOCs and other security prototypes.

Each subsystem has its own visualization module (HMI)

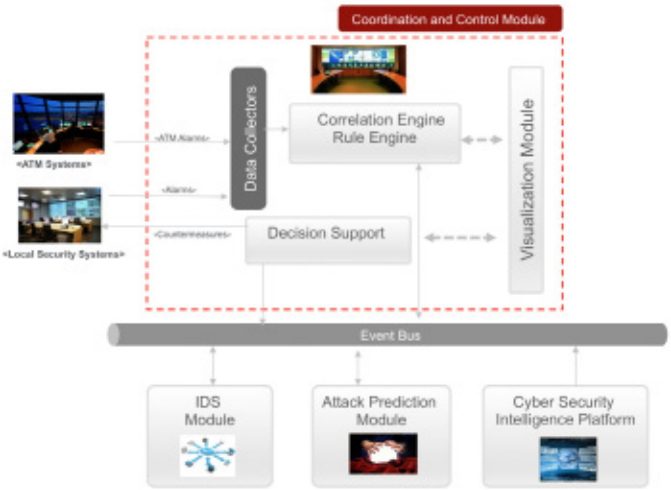


Figure 2: SMP architectural lay-out.

that is included in the Visualization Module of the Command and Control subsystem.

SMP receives input from:

- Local Security Systems (LGSOC or other Prototypes) (security events / detections)
- ATC systems (alerts from systems within the ATM domain)
- Other SMPs (disseminated alerts / messages)
- The internet (open source information about possible attacks in social networks, chats, etc.)

SMP outputs are:

- Security reports (to Local Security Systems or to other SMP)
- Correlated alarms due to the correlation function
- Recommended Countermeasures (to Local Security Systems or to other SMP)
- Attack effect prediction reports (to Local Security Systems or to other SMPs)
- Alarm clearing (to some other Prototypes)

The following paragraphs describe the Security Management Platform main functions

B. Command and Control subsystem

This subsystem provides Alarm Correlation, Security Monitoring and Decision Support for Incident/Crisis Management.

It includes a Data Collector for gathering security events from Local Security Systems and ATC systems, correlating them using a Correlation Engine and displaying the resulting alarms to the operator with the Monitoring facility.

A decision support function allows the operator to provide possible countermeasures to Local Security Systems or other SMPs.

A sanitization function is also available in order to opportunely modify sensitive information before transferring them to the IDS module for dissemination.

C. Cyber Security Intelligence Platform

The Cyber Security Intelligence Platform (CSIP) is based on an open source intelligence service provided in cloud by Finmeccanica. The intelligence module is connected to the Command and Control module by API connection .

CSIP provides GAMMA operators the possibility to obtain relevant information about possible (cyber) attacks on ATM systems, crawling the internet though open sources such as social networks, in order to determine the sentiment and/or threats related to a particular target. They also allow to identify the motivation, the characteristics and the identities of the attackers.

The main functions of CSIP are listed below:

- Intelligence Scenario Configuration
- Crawling of RSS, Twitter, Facebook, PAD
- Indexing & Searching
- Sentiment analysis
- API for Security Reports exportation
- e-mail alerting possibility

The tools available for the operator are:

- **Searching** semantic search of information system impairments, such as cyber attacks and data breach
- **Dashboards**: customized dashboard to provide aggregate views according the specific analyst needs
- **Case Manager**: visual analysis of complex situations
- **Reporting**: automatic report generation related to either corporate data subtraction or any detected attack under preparation (pre-planned attack)

Having defined a scenario of interest described by the specification of patterns, keywords and a time interval, the GAMMA operator using an advanced mechanism of crawling and analysis, can acquire data from monitored sources, identify patterns related to the particular scenario and extract generic or specific entities. The processing of the data found in this way allows then to obtain meta-data information, which will be subsequently used for analysis.

The results of investigations conducted are immediately usable by analysts through the dedicated dashboard.

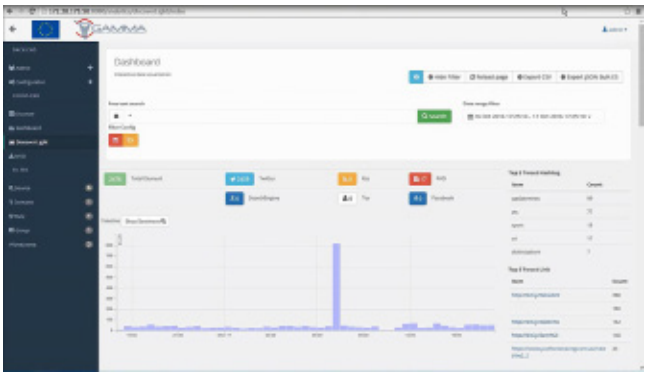


Figure 3: CSIP dashboard.

Once relevant information is obtained, the GAMMA operator can produce a Security Report that can be sent to connected ATM domains and disseminated (through the IDS module) to other SMPs at national or European level.

D. Attack Effect Prediction Module

As was stated before, the SMP serves as a central collector and analyzer of the information generated by diverse set of security controls and event detectors. In this case the joint and sequential analysis of the received information may serve a crucial task, as the Data Fusion enabled by the SMP may reduce the number of false alerts [6] and enable temporal analysis of the actions of the adversary.

The Attack Effect Prediction (AEP) Module is a decision support SMP sub-system that provides a joint assessment of the information received from different sensors (event detectors) represented at the system.

Received information is used to address the following problems:

- Is the system under attack?
- What is the qualification/skill of the adversary?
- What are the targets selected by the adversary?

In order to resolve the stated problems, the overall system should be formally described.

As a system descriptor a directed graph structure is used, following the approach used in Network Security Games (NSG) [7].

The graph encodes all Supporting Assets (SA) as a subset

of nodes and all threat scenarios as a set of paths to the SAs, that form the graph.

Additionally, an impact value for each type of attack for each security control is given (or a set of values for different Impact Areas).

Security controls and event detectors are linked to the nodes of the graph.

The model assumption is that the adversary selects a subset of paths to the SAs and security controls and event detectors may mitigate the impact values or detect

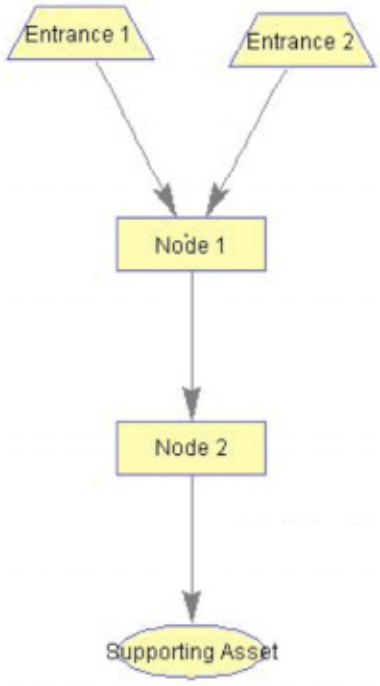


Figure 4: Example of the graph model.

the attacker's actions.
Using the proposed graph model formalization, the state of the adversary may be described as a tuple (P, S, T). P stands for the position (node in the graph), which may be empty in case of no attack taking place. S is the skill-vector of the adversary, which describes the ability to overcome the security controls. T stands for the targeted SA by the attacker.

Thus, the system estimates the state of the adversary for each moment of time given the received event detections.

Parameters P, S of the adversary's state are estimated using Dynamic Bayesian Network for sequential data analysis, which is similar to the approaches used for Bayesian Multiple Target Tracking [8].

The AEP system updates its' internal parameters using newly received information for each moment of time, similar to the correction step of Bayesian Filters, updating the adversary's state beliefs (probability distribution). Parameter T is estimated based on game theory methods.

From the estimated probability distribution over adversary's state a subset of most probable states are selected.

An expected impact is estimated for each of the selected states, based on the predefined impact values, estimated adversary's skills and implemented security controls' properties. Derived information is reported to the overall system via the Event Bus.

E. Information Dissemination (sub)System

The Information Dissemination System (IDS) is an open architecture platform and can interact with a multitude of event sources. In the scope of GAMMA it receives security information from other modules within the SMP over an Event Bus (using the open messaging system product Kafka from the Apache Software Foundation [5]). The information is retained within the IDS and can be accessed by the user.

IDS facilitates manual as well as automatic dissemination of security information to other stakeholders at national or European level.

Each IDS instance of SMPs at national level is connected to the IDS instance of the SMP at European level. When IDS instances are up and running, a network (see Figure 5) is built up between SMP's to share the security information.

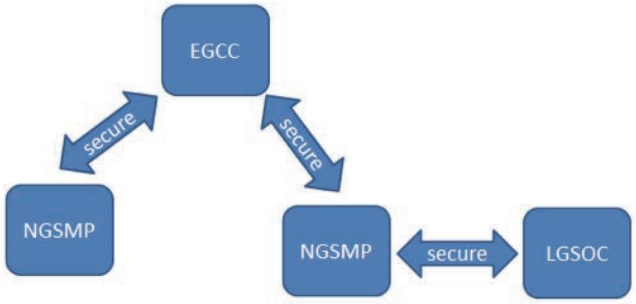


Figure 5: Network of SMP nodes.

All the received security information within IDS will be disseminated to one or more involved stakeholders (at local, national and/or European level) on an need-to-know bases by applying dissemination rules on the content of the security information, the source and the expected destination.

After applying the dissemination rules on the security information the designated SMP nodes are known and the encrypted security information will be sent to these designated nodes.

These SMP nodes receive, store and forward the security information via their Event Bus to the other modules within their SMP node domain.

Other than disseminating security information between nodes coming from other SMP modules, the Information

Dissemination System provides situational awareness - in both the temporal and positional domains - of (potential) incident related information (e.g. alarms, security information, intelligence information) received from connected detection systems.

It is based upon the views presented to ATCA in the scope of Civil-Military Cooperation [4].

The information is presented on a concise situational awareness display (see Figure 6) with the possibility to zoom to the infrastructure level or system level.

The IDS provides the means to embellish the situational display with dynamic information (e.g. traffic, weather, etc.) from external systems.

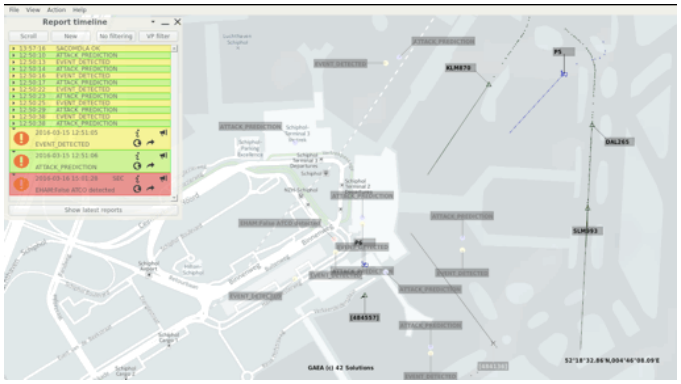


Figure 6: IDS Situational Awareness Display.

Within GAMMA, IDS demonstrates the inclusion of the air traffic picture based on ATM data coming from external track and flight data sources.

The situational awareness display provides several maps to support concise situational awareness fitting the corresponding level of detail.

V. MULTILEVEL IMPLEMENTATION

As mentioned above GAMMA establishes three different levels for managing security:

- the European level represented by the European GAMMA Coordination Centre (EGCC),
- the National level represented by the National GAMMA Security Management Platform (NGSMP)
- the local level represented by local security systems, namely “Local GAMMA Security Operation Centers” (LGSOC).

In terms of instantiations of the SMP this kind of approach foresees:

- one SMP instance in the EGCC
- one SMP instance for each NGSMP

The SMPs at national level are connected to the SMP at European level through the IDS modules.

Each SMP at national level is connected to national Local Security Systems and ATM systems.

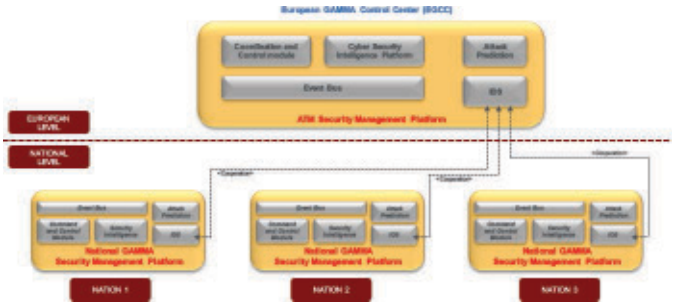


Figure 7: The SMP implmentation in the multilayer approach.

VI. A VALIDATION SCENARIO

The overall objective of the validation work package of the GAMMA project is to validate the GAMMA Security Management concepts, together with their related operational scenarios, procedures and developed technologies.

An example of the various scenarios that have been prepared for validation purposes is the one illustrated in figure 8.

This scenario is related to the dissemination of (sanitized) information from NGSMP level to EGCC level, providing possible countermeasures to Local Security System about an ongoing attack.

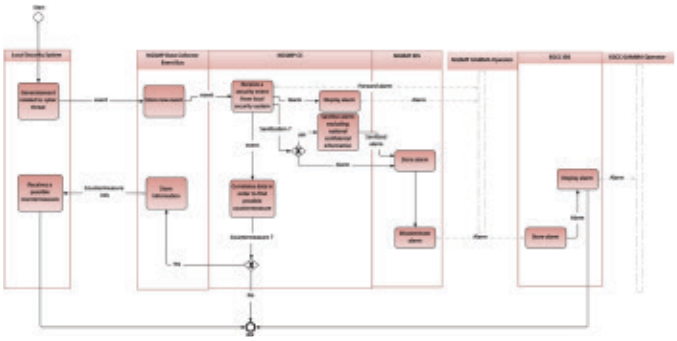


Figure 8: Validation scenario of SMP prototype.

A security event is sent form a Local Security System to the National GAMMA Security Management Platform (NGSMP) and displayed as alarm by the monitoring function of C&C module. The GAMMA operator decides to forward the alarm information to the EGCC.

Before forwarding, he “sanitizes” the information eliminating parts not permitted by national dissemination policies.

The sanitized alarm is sent through IDS module of NGSMP to European level and is displayed by the Monitoring function of the SMP instance of the European GAMMA Control Center.

Furthermore, using the Decision Support function, the GAMMA operator at NGSMP level send to the Local

Security System a possible countermeasure for the security event.

VII. CONCLUSIONS

The most important concept of the GAMMA project, implemented by the federated architecture of the Security Management Platforms, is the sharing of security information between ATM stakeholders.

The SMP architectural vision enlarges the scope for cooperative management of ATM security while assuring controlled sharing of information, which is fundamental for its acceptance in a multinational context

The GAMMA concept opens the way for managing ATM security at European level, proposing (but not enforcing) recommendations on actions or measures to be taken at lower levels, in line with existing principles of national sovereignty and responsibilities over security issues.

The SMP is an enabler for the implementation of this concept, and can be adopted for the management of ATM security as well as the management of security in any federated environment (i.e. military domain)

REFERENCES

[1] GAMMA Consortium – Description of Work – Part B – September 2013

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

[3] GAMMA Consortium D6.3 Prototypes design and development, 1st release – March 2016

[4] National Security, When Time is of the Essence, Strijland W, 42 Solutions, ATCA Conference Proceedings, Winter 2014: www.atca.org/2014-Conference-Proceedings

[5] Apache Kafka: www.kafka.apache.org.

[6] Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management, Shahbazian, E., Rogova, G., Valin, P, ISBN print 978-1-58603-536-5.

[7] Models for nuclear smuggling interdiction. IIE Transactions, Morton, D.P., Feng, P., J., S.K. 39(1), 3–14 (2007).

[8] Sonar tracking of multiple targets using joint probabilistic data association, T. Fortmann, Y. Bar-Shalom, and M. Scheffe, IEEE Journal of Oceanic Engineering, vol. 8, no. 3, pp. 173–183, July 1983

EMAIL ADDRESSES

claudio.porretti@finmeccanica.com

raoul.lahaije@42solutions.nl

denis.g.kolev@gmail.com

ATTACK PREDICTION MODEL FOR FUTURE ATM SYSTEMS

D.Kolev *and* ***G.Markarian****, Lancaster University, UK*

Current **practices and standards for security risk management** involve the identification of **security risks** and the **implementation of associated controls** at a system- or component-level. The risk assessment is typically performed by experts and based on a mix of qualitative and quantitative methods. However, the higher levels of interconnectivity across infrastructure components require the **analysis of threat propagation within and across the associated supply chains**. There exists a wide variety of security risk management methodologies, but few are specifically tailored to the design and development process and to the best of our knowledge, no reliable methodology is available yet for risk management on services involving complex infrastructures such as the health system.

Given the high amount of variables and interdependencies involved, it is essential to employ analytics to assist the process of risk management and evaluation in ATM systems and infrastructures. Deployment procedures include installations (both public and private that need appropriate security levels), that are planned beforehand, in parallel with the development process. That kind of procedures are often projected using an applied mathematics approach for security, usually derived from the domain of probabilistic models and multi-agent models.

Probabilistic modelling is used in order to capture the uncertainty of the observed data, which may be caused by unpredictable factors or by the model inaccuracy, in parallel with the general dependency of the observed factors. Such systems may be employed for security/safety objectives to infer the "hidden" global values, that describe the general state of the ATM system, for instance different failure conditions. **Multi-agent models** are especially relevant for the systems that are used for behavior modelling, recommendation, and decision support.

One of the deliverables of the GAMMA project is a novel attack prediction model specifically developed and optimized for future ATM systems. The developed **Attack Effect Prediction Module (AEPM)** is designed using both of the methodologies, where **Probabilistic Bayesian inference** is used for current state estimation and **Game Theory** is used to perform the prediction based on the estimated characteristics of the adversary. The protected ATM infrastructure is modelled using graph-based approach, that is similar to the Attack Trees method and Network Security Games, that encodes the main steps required to perform an attack. The developed model may be considered as a synthesis of the attack scenarios, defined for the protected system and throughout the GAMMA project numerous predefined security threats were analysed and simulated. This allows the graph instantiation procedures to be interlinked with the standard SecRAM methodology, which ensures an expert basis for the model. The designed graph links the mathematical formalism and the main definitions used in risk analysis, i.e. Supporting and Primary Assets, Attack scenario, etc.

The design AEPM supports two modes:

(i) dynamic for real-time risk prediction;

(ii) off-line for security audits of ATM systems.

In dynamic mode, AEPM obtains and processes the information received from diverse sensors, placed within the protected system, which are considered as event detectors. It is important to mention that within the scope of the GAMMA project, the AEPM may process the information from systems of different levels of perception (like cyber intrusion detection for high perception or incorrect login attempt for low), serving as Data Fusion engine. This engine can correlate alarms and detections from different heterogeneous sources (idea, similar to bagging from Data Mining). The AEPM uses the received information to estimate the security status of the system ("under attack" flag probability) and characteristics of the adversary, such as abstract "skill" level and possible intention of the adversary. Based on the estimated information and the structure of the graph that describes the system, a prediction of possible actions of the attacker may be inferred.

In off-line mode, the model is applied to a predefined graph corresponding to a given ATM infrastructure and evaluates its security resilience level. The model can be used for optimsing security resilience by recommending optimal locations of even detectors and providing the desired cost/benefit ratio.

Figure 1 bellow illustrates one of the developed graphs emulating ATM computer network infrastructure. In this particular architecture two possible entries for the attacker (top of the graph) and a number of security assets (bottom of the graph) are defined. All the possible paths from an entry to a security asset are monitored by event detectors and the system calculates the instant probability of an attack.

As it follows from this figure, the developed model provides real time probability of an attack from all current users of the infrastructure. In addition, the initial problem statement may be significantly explored, by enhancing the structure and the space of the adversary's skill variable, incorporating the dependency model between different event detectors.

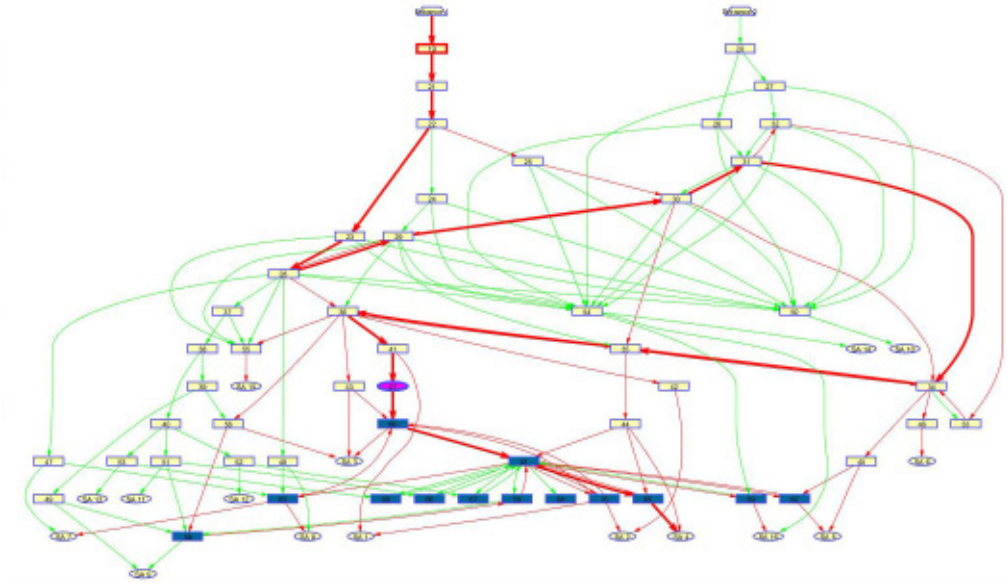


Figure 1: Graph model mapping interdependencies and potential outcomes

Information Dissemination System

42 Solutions

I. INTRODUCTION

The GAMMA vision is to adopt a holistic approach to assess ATM security, in line with SESAR. GAMMA objectives are to:

- Develop a Global ATM Security Management framework, representing a concrete proposal for the day-to-day operation of ATM Security and the management of crises at European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.
- Design and implement prototype components of the GAMMA solution so as to demonstrate the functionalities and operations proposed for the future European ATM.
- Set up a realistic validation environment, representative of the target ATM solution, through which to perform validation exercises aimed at validating the feasibility and assessing the adequateness of the procedures, technologies, and human resources issues proposed.

II. THE CONTEXT

ATC currently relies mainly on verbal communication in crisis situations between stakeholders. One of the approaches within GAMMA is to continuously share security information among the different ATM actors, providing overall situational awareness of the security status of the ATM as a whole, as well as a basis for identifying threats through extended correlations of isolated incidents.

As part of the work performed in GAMMA the following improvements were identified in the area of verbal communication during crisis situation:

- Improvement IMP-DL-REPORT: Exchange of ATM incident-related information between civil and military via data link
- Improvement IMP-STD-REPORT: Harmonisation of information standards and reporting procedures about incidents

III. THE CONCEPT OF OPERATIONS

The GAMMA Concept (see Figure 1) has been defined having in mind principles and concepts related to Security Management in a collaborative multi stakeholder environment.

The GAMMA proposed solution contains a network of distributed nodes (see Figure 2). Each node is embedded within the ATM system and is providing interfaces to (ATM) internal and external security stakeholders. The Information Dissemination System is a module of the Security Management Platform prototype (SMP), enabling the dissemination of security information through the multilevel architecture as proposed by the GAMMA solution.

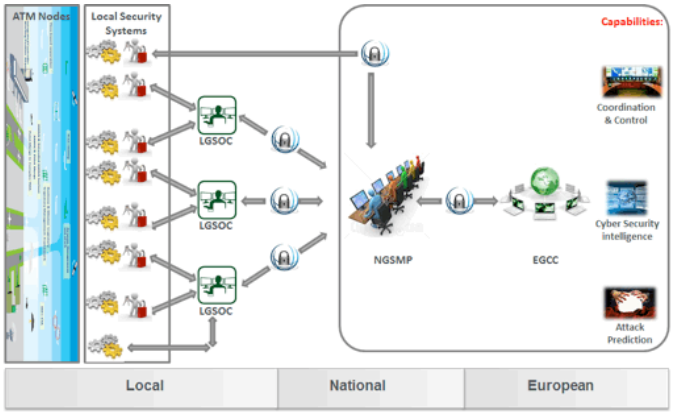


Figure 1: The GAMMA Concept

IV. INFORMATION DISSEMINATION SYSTEM CONCEPT

The Information Dissemination System (IDS) is an open architecture platform and can interact with a multitude of event sources. In the scope of GAMMA it receives security information from other modules within the Security Management Platform (SMP) over an Event Bus (using the open messaging system product Kafka from the Apache Software Foundation). The information is retained within the IDS and can be accessed by the user.

The IDS platform facilitates the secure cross-SMP information dissemination. Each IDS instance connects to one or more other SMP. IDS nodes form a network (see Figure 2) between SMP's to share the security information.

All received security information within IDS will be disseminated to one or more involved stakeholders (at local, national, military and/or European level) on a

need-to-know bases by applying dissemination rules on the content of the security information, the source and the expected destination.

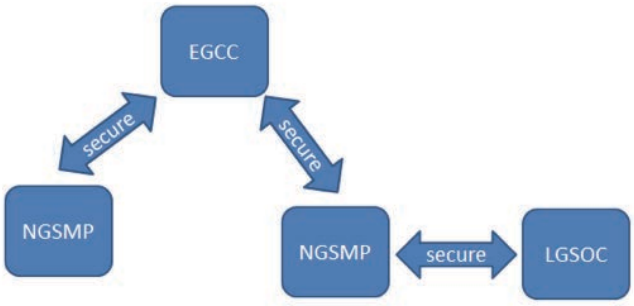


Figure 2: Gamma network of distributed nodes

After applying the dissemination rules on the security information the designated SMP nodes are known and the encrypted security information will be sent to these designated nodes.

These SMP nodes receive, store and forward the security information via their Event Bus to the other modules within their SMP node domain.

Other than disseminating security information between nodes coming from other SMP modules, the Information Dissemination System provides situational awareness - in both the temporal and positional domains - of (potential) incident related information (e.g. alarms, security information, intelligence information) received from connected detection systems. It is based upon the views presented to Air Traffic Control Association (ATCA) in the scope of Civil-Military Cooperation [1].

The IDS provides the means to embellish the situational display with dynamic information (e.g. traffic, weather, etc.) from external systems.

Within GAMMA, IDS demonstrates the inclusion of the air traffic picture based on ATM data coming from external track and flight data sources. The situational awareness display provides several maps to support concise situational awareness fitting the corresponding level of detail to support and expedite incident response management.

V. ARCHITECTURE OF IDS

The IDS architecture consists of the following components (see Figure 3):

- The Event Bus Connector component interfaces with the other SMP modules responsible for the XML decoding / encoding of incoming/outgoing reports and requests/responses.

- The Store component stores all reports and ATM data (tracks and flight plans) received by IDS, correlates reports with other reports and ATM data. It forwards disseminated reports to the Event Bus Connector component and/or the Network Node component for dissemination to the other SMP modules.

- The Situational Awareness Display component displays the reports and ATM data on temporal and positional domains.

- The Dissemination component contains the dissemination rules for connected SMP nodes within the GAMMA WAN and determines based on the dissemination rules whether the reports are granted for one or more of the SMP node(s).

- The Network Node component disseminates the reports to the target connected SMP nodes.

- The ATC Connector component is the interface with ATC network.

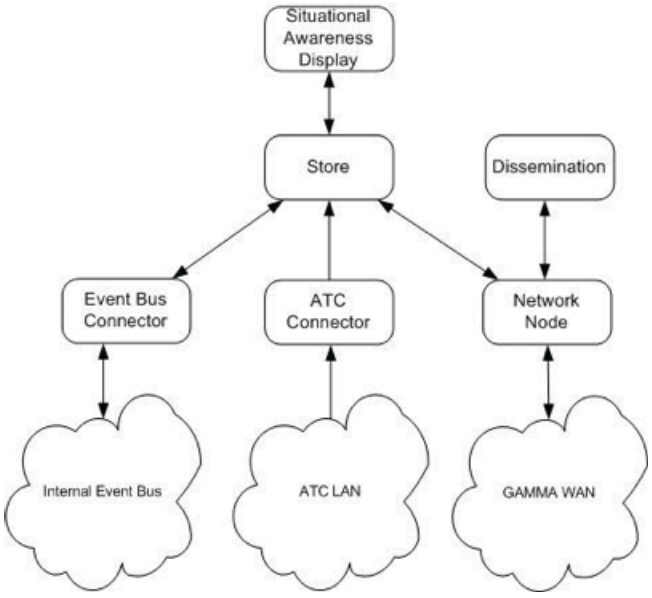


Figure 3: IDS components

VI. VALIDATION ACTIVITIES

The overall objective of the validation work package of the GAMMA project is to validate the GAMMA Security Management concepts, together with their related operational scenarios, procedures and developed technologies. The IDS module as part of the GAMMA Security Management is validated within partial integration 1(PI1) and full integration 3 (FI3) validation exercise.

The partial integration1 validation scenario shows a hijack and an attack on the on-board SATCOM equipment of the aircraft and a close coordination via voice and via datalink between civil and military authorities. The attack on the on-board SATCOM triggers an alarm on the last known position on national level and based on this information

the national authorities decide to disseminate the alarm to the military authority using IDS (see Figure 4).

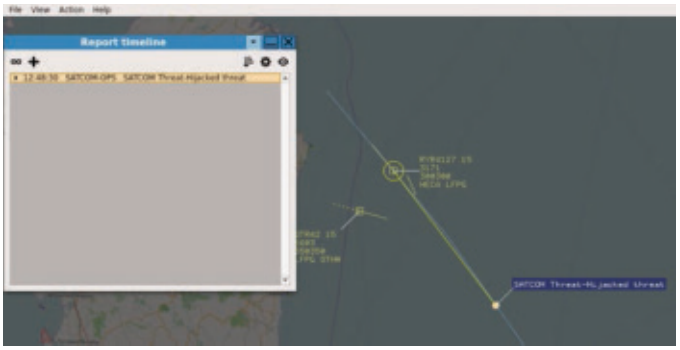


Figure 4: IDS in PI1 validation exercise

The full integration 3 validation scenario (see Figure 5) shows coordinated and uncoordinated attacks (SOAP/ https security attacks on SWIM, on-board attacks on the aircraft systems) in 2 countries. At European level it is decided to inform a third country about these attacks using IDS.

VII. CONCLUSIONS

Within GAMMA a basis for standards has been laid down for information sharing, but a harmonised information standard is not yet defined and will represent a challenge for a follow up project.

REFERENCES

[1] National Security, When Time is of the Essence, Strijland W, 42 Solutions, ATCA Conference Proceedings, Winter 2014: www.atca.org/2014-Conference-Proceedings

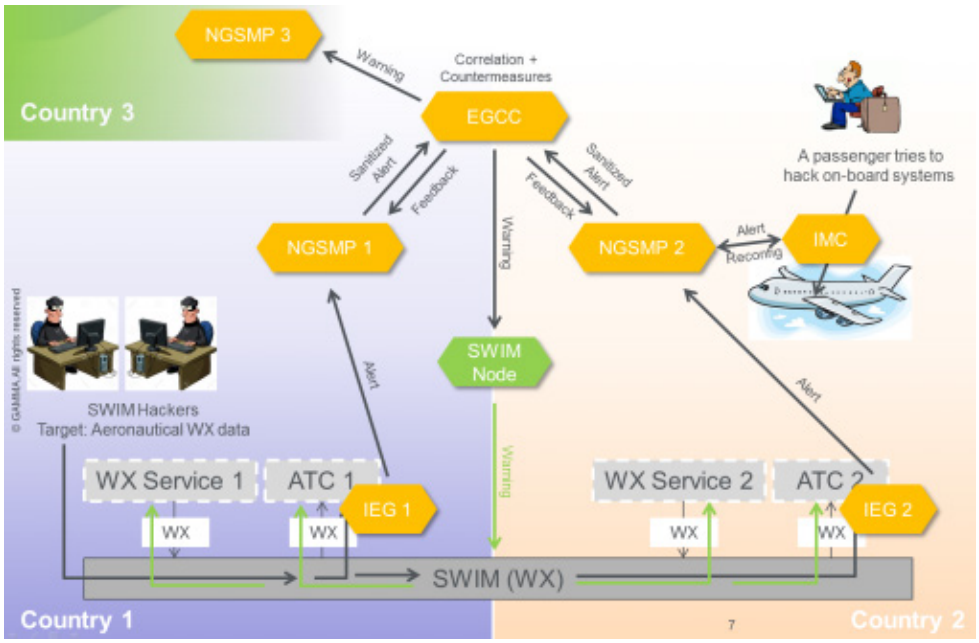


Figure 5: FI3 validation scenario

The Secure ATC Communications Prototype

DLR

INTRODUCTION – STATE OF THE ART

Air Traffic Control (ATC) is the base for today's worldwide air traffic. Having its beginnings in the mid 1940's, this service is being provided according to very mature standards issued by the International Civil Aviation Organization (ICAO). The overall goal of air traffic control service is to prevent collisions between two aircraft, between an aircraft and another object or between aircraft and ground structures and terrain. Safety is the highest asset in aviation.

Basically, ATC service can be subdivided in three categories:

- Aerodrome Control Service, being responsible for all aircraft landing and taking off at a controlled airport, ground movements of aircraft and vehicles at a controlled airport and aircraft flying in the vicinity of controlled airfields. This service is provided by an Aerodrome Control Tower.
- Approach Control Service, being responsible for all aircraft approaching or departing a controlled aerodrome by complying with Instrument Flight Rules (IFR). This service is provided either by a local approach control unit or from a working position in an Area Control Center, depending on the country.
- Area Control Service, being responsible for all aircraft complying with IFR during their enroute phase. This service is provided by several working positions in an Area Control Center.

Figure 1: Aerodrome Controllers at Munich Airport (Source: DFS Deutsche Flugsicherung GmbH)

SECURITY RISK IN PILOT-ATC VOICE COMMUNICATION

All kinds of ATC service have in common that they are still performed by using 'outdated' analogue VHF radio transceivers to establish communication between air traffic controllers and pilots. Voice communication has many advantages and is still the most flexible and most efficient way for controllers of communicating with, giving clearances to and getting feedback from pilots.

But one significant disadvantage of analogue VHF radio communication is that this system was never designed to be a secure line. There is no possibility to easily apply encryption algorithms on an analogue signal. Analogue VHF transmissions are totally unprotected and can easily be eavesdropped, jammed or imitated. Technology to protect wireless communication channels from unauthorized access is already available, but not applicable as analogue VHF radio communication is such a basic standard in aviation that it is very challenging to introduce any changes in this world wide air traffic network. This opens the door for a threat called "False ATCO" scenario: a person giving fake ATC clearances to pilots with the goal to severely hamper the safety of air traffic; maybe even to provoke a collision between two aircraft. To counter this threat a system is needed which secures the air-ground voice communication without any technical modification of the used communication technology.

THE SACom CONCEPT

One of the seven prototypes developed within GAMMA exactly addresses this issue: the Secure ATC Communications Prototype (SACom). This prototype is designed as a system which continuously monitors the air-ground voice communication, the behavior of all aircraft under control and the relative positions of all aircraft to each other. As this system shall not intervene in the existing air-ground voice communication it can be seen as an assistance tool for operators. The SACom prototype raises the situational awareness of controllers and pilots and enables them to directly identify unauthorized transmissions and/or the consequences of successfully infiltrated fake ATC clearances. Such consequences are most likely aircraft deviating from their valid ATC clearances or aircraft which do not (fully) comply with new valid ATC clearances.

The SACom prototype does not just have one single security function to detect unauthorized clearances. In fact the SACom prototype combines and correlates several indicators of a different kind to achieve a greater robustness, a higher flexibility and to be able to determine whether an incident or event has a security or a pure safety background. Security events always involve some kind of intentional disturbance, which may be precisely targeted at known weak points while safety events are driven by chance and can usually be clarified as soon as they are detected.

The different SACom indicators are:

- Speaker verification by means of voice analysis: The voice of all speakers is compared to known voice patterns of all authorized speakers. This function directly detects unauthorized transmissions.

- Stress detection by means of voice analysis: It can be expected that all speakers which are consciously exposed to unlawful interference show a higher level of workload, tension and confusion, which leads to a higher level of stress. This function detects a symptom of attempted or successful unauthorized transmissions.

- Conformance monitoring: The behavior of all aircraft is continuously compared with valid ATC clearances to detect any undesired behavior or deviations. This function detects a symptom of successful unauthorized transmissions.

- Conflict detection: Given ATC clearances are continuously cross-checked against the current traffic situation to detect possible conflicting ATC clearances. This function acts as an advanced safety net.

THE ARCHITECTURE OF THE SACom

These different functions are contained in three different SACom modules: the Speaker Verification Module (SVM) which houses the speaker verification function, the Stress Detection Module (SDM) which houses the stress detection function and the Conformance Monitoring Module (CMM) which houses both conformance monitoring and conflict detection functions. SVM and SDM need direct access to the air-ground voice communication audio stream as well as to a database of known and authorized speakers. The CMM needs access to the air traffic situation (radar data) as well as valid ATC clearances. SVM and SDM were developed and finalized by the Slovak Academy of Sciences (SAV) in Bratislava, Slovakia. The development of the other SACom modules as well as the assembly of the prototype was performed by the German Aerospace Center (DLR), located in Braunschweig, Germany.

In addition to that, the SACom has a fourth module correlating and weighting the outputs of the other three ones, which is called Security Management Interface (SMI). This module can provide an overall security indicator score, which can be used to judge if an event has a security or a pure safety background or for automatic reporting functions to a Security Management Entity, such as the Security Management Platform, which is developed by Leonardo.

The following figure illustrates the SACom architecture.

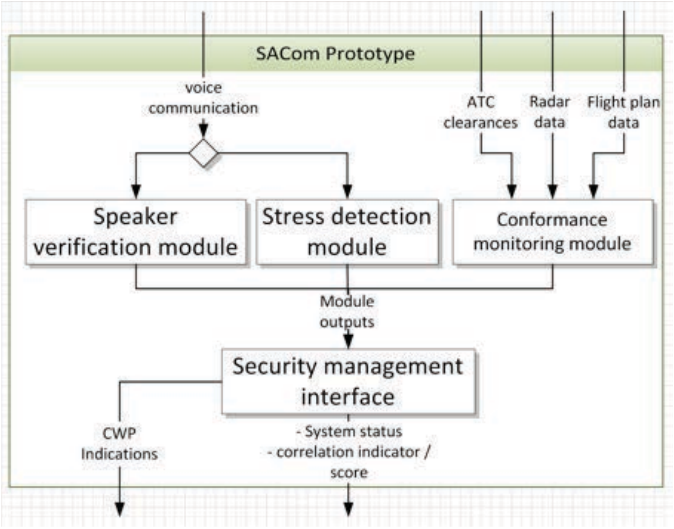


Figure 2: SACom Prototype Architecture

VALIDATION ACTIVITIES

The SACom prototype was validated by DLR in October 2016, involving 6 active air traffic controllers. During the validation trials, several ATC simulations were performed which contained on one hand specific situations which may be caused by a “False ATCO” interference. On the other hand a complete attack with several fake ATC clearances was simulated in a very realistic way. This simulation campaign showed the usability of the SACom prototype and brought up many insights in the nature of such attacks and how well the air traffic controllers of today are prepared to such events. It is expected that the complete results will be published in 2017.

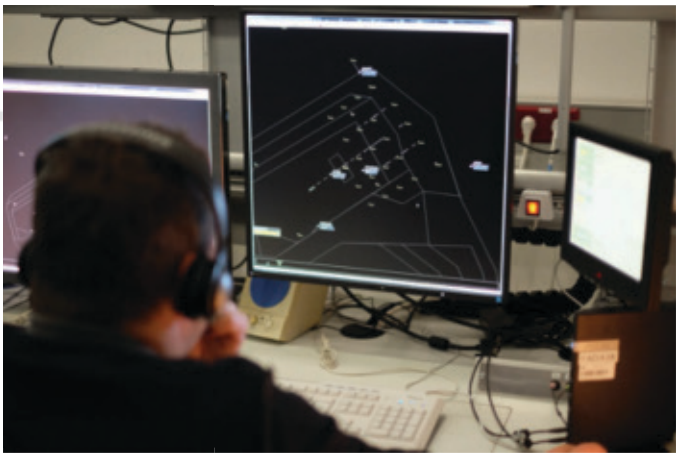


Figure 3: Air Traffic Controller testing the SACom during Validation Trials in 2016

TOWARDS A MORE SECURE ATC VOICE COMMUNICATIONS SYSTEM

*Tim H. Stelkens-Kobsch, Dr. Andreas Hasselberg, Dr. Thorsten Mühlhausen, Dr. Nils Carstengerdes, Michael Finke and **Constantijn Neeteson**, German Aerospace Center (DLR), Braunschweig, Germany*

ABSTRACT

Contradictory to communication safety in the aviation field communication security has received relatively little attention to date, although the threats regarding air traffic security have been rapidly increasing in recent years. Within the project GAMMA (Global ATM Security Management) the German Aerospace Center (DLR) is developing a prototype to support air traffic controllers (ATCO) in detecting intrusions into the air ground voice system and therefore allow subsequent mitigating actions to be conducted.

INTRODUCTION

Many significant accomplishments to secure Aviation have been reached in the last years. While much effort was spend to address the physical security, threats against its information infrastructure are not well covered [1]. For example the pilot-controller very high frequency (VHF) voice communication is open to masquerading intruders, which pretend to be air traffic controllers and give instructions to aircraft. While the problem has cached the interest of some researches [2] and was identified as threat in a study by Eurocontrol [3], it has not really attracted community's attention so far. On one hand this results from not causing crucial damages until now, on the other hand this is induced by the cautious policy of ANSPs (Air Navigation Service Providers). However, there is a significant number of attacks [1] and examples demonstrate, that they pose a real danger of confusing air traffic controllers and pilots [4] [5].

This paper describes the approach to develop a dedicated prototype for secure ATC communications, the risk assessment and the risk treatment regarding ATC communications as conducted in the ongoing GAMMA project using SESAR's methodology [6] and applying SESAR's Minimum Set of Security Controls (MSSC) [7].

In order to establish the context, the first part of the paper will describe the investigated system which is currently in use for air-ground radio communications in ATC. Further, the applied methodology to assess and treat the risks regarding the air-ground radio communication system will be explained. This will lead to the postulation of a prototype which will be built within the project GAMMA in order to increase resistance against the elaborated threats and to reduce the vulnerability of the system. Finally, the approach to evaluate the benefit of this prototype will be described and the paper will be completed with a discussion about the next steps and an outlook to the future.

AIR GROUND COMMUNICATION IN AIR TRAFFIC CONTROL

In the present time, air-ground communication between ATC and aircrews is designated as 'aeronautical mobile service' as part of the 'international aeronautical telecommunication service'. Within the aeronautical mobile service, voice communications and data link communications can be distinguished [8]. For now data link communications are already implemented as CPDLC (Controller Pilot Data Link Communications) for exchanging messages in a non-time critical context. Further extension of using data link communications can be expected in the future. But due to several operational problems especially in a busy 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 the aeronautical mobile service.

From the technical point of view, voice communication in aviation is done by using omnidirectional analogue radio transceivers. Civil ATC radio communication uses the VHF band within 117.975-137.000 MHz. Carrier waves are double-sideband and amplitude modulated. ATC ground stations work with a higher power output than airborne stations and are designed to ensure sufficient radio coverage depending on operational demands [9]. ATC voice communication equipment has to be protected from unauthorized access in general [8].

Radio transmissions have specific wave propagation characteristics depending on the frequency, transmitter environment and transmitting method (directional, omnidirectional, etc.). VHF (Very High Frequency) transmissions require a radio line-of-sight to a certain extend; wave deflection effects play a minor role. This leads to the consequence that communication between two ground stations or between a ground station and

a low flying aircraft might not be possible, depending on the distance and topography between them (Figure 1). Further, due to the omnidirectional transmission, the signal power decreases with distance, leading to a reduced communication quality with increasing distance due to background noise. Consequently, transmissions from distant stations can more easily be blocked out by other nearby stations.

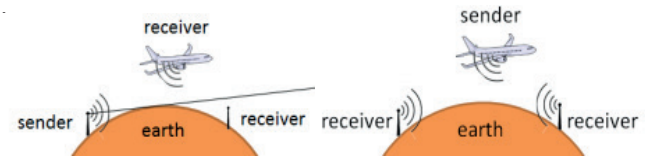


Figure 1: Line of Sight Dependency for VHF Transmissions. Left: Ground Receiver Does Not Track Sender. Right: Both Receivers Track Sender.

Depending on national regulations, VHF transmitters may only be operated with a specific approval by a national authority [10].

To take part in air-ground voice communications, a special knowledge regarding voice communication procedures and standard phrases as well as a sufficient language proficiency is required. Also depending on national regulations, a radio telephony certificate may be obligatory [11].

With regard to security, the air ground voice communication can easily be intruded due to general availability of aircraft radio transmitter equipment and its analogue, unsecured nature.

RISK ASSESSMENT

The overall process of risk identification and risk evaluation is called security risk assessment [12]. After assessing risks, it is possible to identify a set of security requirements which ensure that the consequences of an attack are known and managed and that the targeted asset can recover to normal operations in a reasonable time. The required main phases for the assessment of security risks are typically [12] (cf. Figure 2)

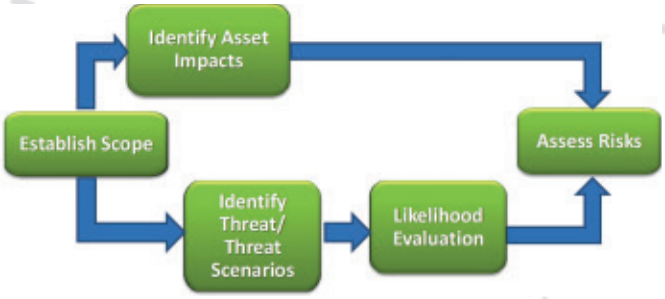


Figure 2: Typical Security Risk Assessment Process [13].

- to establish an accurate scope,
- to identify asset impacts,
- to identify threats / threat scenarios,
- to evaluate the likelihood of each threat / threat scenario,
- to assess the security risk.

When this process is completed it is followed by the definition of a set of security controls (treatment actions) and requirements to reduce the risk level of unacceptable risks to an acceptable level.

In the frame of SESAR a step-by-step guidance was developed which provides support for an operational focus area (OFA) to use the security risk assessment methodology (SecRAM). In Figure 3 the steps to execute the SecRAM methodology proposed by SESAR are represented graphically.

In the context of secure ATC communication the SecRAM methodology was applied to the air ground communication system currently used in air traffic control as described above.

This approach will be further described in the following sections (see also Figure 3).

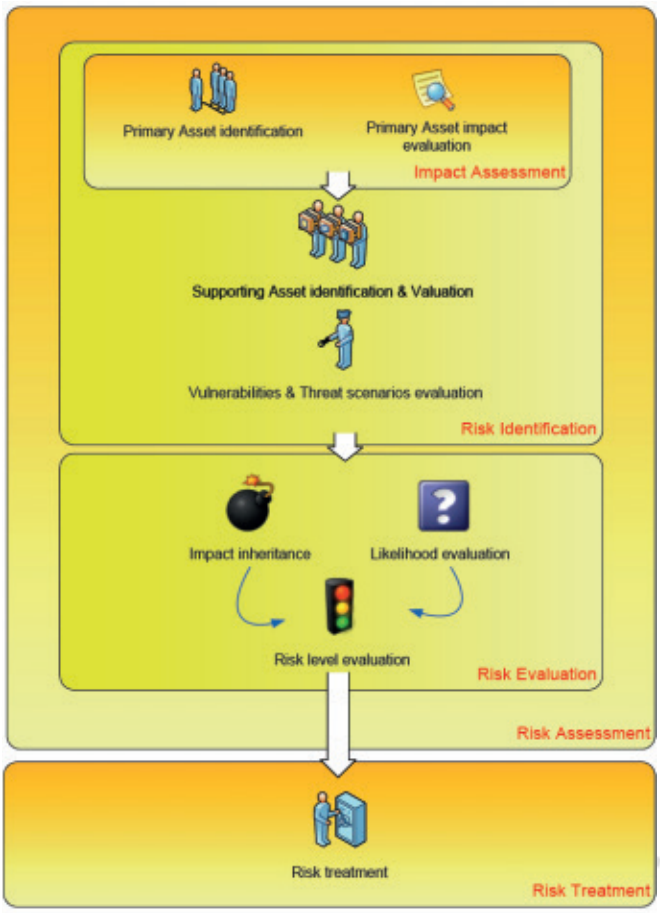


Figure 3: SecRAM Methodology [13].

Asset Identification and Valuation

The differentiation between primary assets and supporting assets has to be defined in advance of performing a risk assessment. Following [12], primary

assets are for example intangible information and services which are of value to an OFA and which shall be protected. A successful attack would ultimately impair the primary assets and have an impact on the ATM system.

Supporting assets are entities which enable the primary assets. Supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets.

Primary Asset Identification

There are two types of primary assets which have to be protected: services and information (more precisely primary information).

Services may be further divided into services addressed by the OFA, system services, operational concepts and operational activities which are essential to keep the business mission running (solely or in combinations), contain secret processes or involve proprietary technology. Furthermore the necessary services to comply with contractual, legal or regulatory requirements have to be secured.

Information is considered as primary when it is (1) vital for the exercise of the mission or business, (2) personal regarding privacy issues, (3) strategic and/or confidential, (4) high-cost belonging to long time acquisition duration and/or high acquisition cost.

Impact Assessment

For each primary asset the required level of Confidentiality (C), Integrity (I) and Availability (A) has to be defined. Typically this is achieved by stating a number from 1 to 5 for each of the CIA criteria allocated to the asset. Thereafter, the impact regarding loss or degradation of the above stated criteria has to be evaluated in case of impact on the considered asset. Within GAMMA this was done using the SESAR security impact areas described in [12].

Supporting Asset Identification and Valuation

As stated earlier supporting assets are tangible elements that support the existence of primary assets. Entities involved in storing, processing and/or transmitting primary assets are classified as supporting assets. Examples are servers, databases, laptops and workstations [14]. When identifying supporting assets it has to be considered that each supporting asset is linked with one or more primary assets.

After applying the SESAR methodology, the supporting assets of the ATC communication system have been identified being the voice system, each individual aircraft, each en-route ACC (Air Traffic Control Center), each approach ACC and each airport tower.

Threat Scenarios

In order to act out possible threats affecting the assets of ATC radio communications, a list of threat scenarios relevant for the OFA has been elaborated. In order to establish the list it was assumed that a threat scenario is the chain of events or occurrences which take place starting with a threat source and ending with the consequences of an incident. The scenario is originated by 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 [12].

Threat Sources Identification

Risk assessment proceeds with the next step which is intended to identify all possible threat sources which may exploit vulnerabilities of supporting assets in order to achieve their aim to compromise the system. Following the SESAR approach the process is performed by starting from two different origins: A vulnerability assessment of all supporting assets and a review of attackers and how they can attack a supporting asset. This step has a valuable impact on the development of security requirements as it is expedient to consider all possible threats to the ATM system. All threats which are not covered in this step will pose a high potential danger on the system, because they are unknown.

Though it is some kind of reading tea leaves the consideration of future threats is an immensely important task within this step of the risk assessment. One technique which shows to be effective in finding out new threats, threat agents and assets into the security viewpoint is horizon scanning [15]. For each time horizon the approach is to determine, detect and collect new threats/attack methods or assets. These time horizons may vary between a short term horizon over medium term horizon to long term horizon.

Threat Scenario Assessment

Within this part several threat scenarios shall be developed covering each selected, potential threat of the OFA. This includes the identification of the attacker and the attacked supporting asset as well as the detailing of the vulnerabilities of the supporting asset and the different means of the attack.

A major outcome of this assessment step is the development of concrete examples describing the threats, the vulnerabilities and the threat sources. The scenarios are described in narrative text and shall be coordinated with stakeholders.

Risk Evaluation

Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or

tolerable. In this context the security risk is a combination of the impact of a successful attack and the likelihood that the impact will be achieved.

Impact Evaluation

The impact evaluation takes into account the situation with and without security controls in place to reduce the impact of an attack. This leads towards two different impacts attacks may have on the considered system: the inherited impact which describes the maximum impact a threat scenario would have without existing security controls and the reviewed impact which is to be expected when existing or planned security controls are taken into account for mitigating the impact of threats on the system. Consequently the reviewed impact is always equal or less then the inherited impact. When the reviewed impact is different from the inherited impact the causing security controls shall be listed and described.

Likelihood Evaluation

Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics). In this part of the assessment the likelihood that an attack is successful shall be estimated. When determining the likelihood the existing and planned security controls have to be taken into consideration. The scale to differentiate the probability of likelihood ranges from very unlikely to certain. This categorization helps to classify the severity of a potential attack resulting from a threat and the impact of a threat scenario on the system.

Risk Level Evaluation

The level of risk is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks. In the practical application within GAMMA this is applied to the generated threat scenarios in order to determine the risk level. For all threat scenarios, the risk level of a threat scenario follows an automatic calculation from the reviewed impact and the likelihood of the threat scenario resulting e.g. from Table I. It has to be mentioned that there are different forms of risk level evaluation tables mentioned in literature but the 5x5 matrix shown in Table I was decided to be the most suitable because of its adoption by SESAR.

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Table 1. Risk Level Evaluation [13]

SECURITY OBJECTIVES

Security objectives are derived from high level OFA policy objectives and are measurable statements of intent relating to the protection of a primary asset [12]. This means that the identified risks on primary assets are used as an input for a so called security objective report. Here the security objectives on primary assets are defined and compared with risk levels in order to decide if a distinct risk should be treated or is acceptable (also referred to as security needs).

Security objectives are again defined in terms of confidentiality, integrity and availability of the associated primary asset.

In order to determine the security objectives regarding the air-ground voice communication system the following approach has been chosen:

The possible impact of feared events on this system has been used to list the security objectives. Security needs, well known as the risk appetite, have then been calculated by confronting the level of risk of the identified threats with the security objectives.

The last step was performed as described in [14]. This step consists of the risk treatment by reducing the risk (with technical or procedural security controls), avoiding the risk (stop the function concerned by the risk), accepting the risk (with its consequences) or transferring it (the risk will be covered by another system/entity).

RISK TREATMENT

Risk treatment (as conducted in [14]) develops a set of security controls to ensure that the remaining residual risks after the risk treatment meets the aforementioned security objectives.

To achieve this, the risk treatment involves selecting and implementing one or more treatment options for identified risks and is therefore a process to modify or manipulate them. Once a treatment has been implemented, it becomes a control or it modifies existing controls. There are four options for risk treatment: risk reduction, risk avoidance, risk acceptance, or risk transfer [13]. The main concept of risk treatment is to select a list of prioritized risks from the risk evaluation step and define a risk treatment plan.

The Security Risk Treatment conducted in GAMMA can be summarized with the following steps:

- Collection of main inputs from the security risk assessment performed,
- Risk treatment prioritization,
- Association of the Minimum Set of Security Controls (MSSC) defined by SESAR to each risk identified,

- Refinement of SESAR MSSC and definition of additional security controls for every asset and threat scenario,
- Residual risk evaluation,
- Additional security recommendations.
- Security Key Performance Indicators (KPI)

One important component of the risk treatment is the application of the MSSC. The MSSC define a set of common-sense controls which all OFAs shall apply. These sets have been elaborated by SESAR [7] and applied during the risk assessment process in GAMMA. All resulting vulnerabilities were then investigated and additional security controls have been postulated which reduce the residual risks to tolerable levels. Thus the outcome of the risk treatment phase was a set of security controls which allow decreasing the vulnerability while increasing the security of the ATC air-ground communication in the best way. The security controls have been further elaborated and resulted in the postulation of a prototype to be hooked up to the existing system.

The discussed prototype for securing ATC communications consists of three detector modules, namely speaker verification module, voice pattern anomaly detection module and conformance monitoring module, and one correlation module (see Figure 4). This prototype will be installed as well on ground in the controller working positions (CWP) of the air traffic controllers as in aircraft cockpits. The speaker verification module listens to the voice communication and identifies the speakers

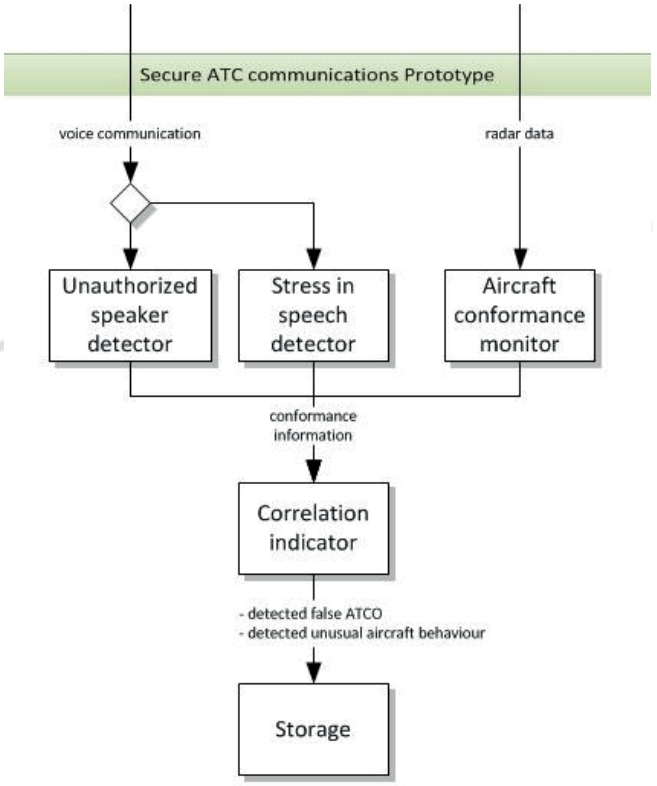


Figure 4: Logical View of a Prototype to Secure ATC Communications.

by comparing the voice signals to a stored acoustic fingerprint. The voice pattern anomaly detection module listens to the voice communication and identifies abnormal voice patterns (e.g. induced by stress). The conformance monitoring tool uses electronically available clearances and radar data as input and checks if the aircraft flight trajectories correspond to the instructions and the predicted regular behaviour.

Additionally, the on-board version of the discussed secure ATC communications prototype is installed in cockpits. It consists of the speaker verification module and the voice pattern anomaly detection module and forwards its results to the likewise configured prototype located in the ATC Center. Based on the information from these sources the correlation module of the secure ATC communications prototype in the ATC Center decides if a false ATCO is detected. When such an intruder is identified, the result is made available to the ATCO and the cockpit crews in this sector.

At this point it has to be mentioned that a prerequisite for a successful implementation of the proposed prototype should be the transition of air-ground ATC communication from analogue to digital technique, which would immensely support the chances of a secure ATC radio communication system.

APPROACH TO BENEFIT EVALUATION

In chapter V, the prototype for secure ATC communications was introduced. This prototype will be validated according to phase V2 of the European Operational Concept Validation Methodology (E-OCVM, [17]) to gain initial feedback regarding its acceptance and its benefit. Whereas phase V0 and V1 of the E-OCVM Concept Lifecycle Model (CLM) define the air traffic management needs and the scope of the concept, phase V2 explicitly addresses feasibility and recommends validating the concept regarding operational user acceptance and operability.

Within the planned validation activities described in this paper, the herein discussed prototype will be validated as a single prototype without connections to other security systems also developed in the GAMMA project.

As the prototype is developed to support certified controllers in the detection of false ATCOs, the validation should provide evidence that the detection of false ATCOs is improved when support by the prototype is installed. Therefore, the first validation objective is to improve the detection of a false ATCO by utilising the prototype. Furthermore, the situation awareness about attacks of false ATCOs should be improved. Thus, the second objective is to validate that the solution leads to a better situational awareness of as well controllers on ground as cockpit crews in the sector regarding occurrence of a false ATCO.

The acceptance of the secure ATC communications prototype by controllers is one of the crucial issues on hand. If it is not accepted, air traffic controllers will probably not use it or may ignore it. They will only accept such a kind of system, if it is useful and trustworthy in their opinion. Therefore, the third objective of the validation is to validate that the performance of the prototype is acceptable (regarding false alarms, correct detection, usefulness and trust)

To collect feedback for the prioritization of further development effort, the prototype should be validated not only as a whole but the individual modules should be assessed each separately. Thus, the fourth validation objective is to compare the impact of individual prototype subsystems on threat management (speaker verification (SV), voice pattern analysis (VPA) and conformance monitoring (CM)).

In order to conduct the validation exercise, some assumptions have to be made about the operational environment, in which the proposed prototype shall be applied.

- MSSCs are considered as already implemented.
- Secure ATC communication prototype is installed at controller and pilot side.
- False ATCO has enough knowledge and the necessary equipment to provide logical instructions to the aircraft.
- ATC clearances are electronically available and can be used as input for the prototype.
- Speaker verification module has access to acoustic fingerprint of pilots and controllers.
- Speech data during validations is of high digital quality (VoIP), the minimal sampling rate and minimal bits per sample will be defined at a later stage.
- Aircraft prototype for secure ATC air-ground communication is able to downlink indicators to ATC and receive uplinked indicators to the cockpit crews in the sector.

A human-in-the-loop real-time simulation consisting of reference and solution runs will be used as a method to validate the improvements regarding the detection of the false ATCO threat by using the proposed prototype compared to current operations.

During these simulation runs, the real air traffic controller will be faced with a multitude of events. These are (1) valid pilot behaviour, (2) pilot error which is not false ATCO induced, and (3) pilot behaviour induced by instructions from a false ATCO (e.g. false ATCO induced readback, unusual trajectory). Furthermore, the possibility of the real controller to hear the false ATCO will be varied. (4) Half of the instructions from the false ATCO will be audible for the real controller. (5) The other part of the instructions of the false ATCO will only be audible for the pilots, but not for the real controller (simulating the radio line-of-sight issues described in chapter II). The following event categories are therefore defined

Event A) Valid pilot behaviour

Event B) Pilot readback error (not induced by false ATCO)

Event C) Pilot behaviour error (not induced by false ATCO)

Event D) False ATCO induced behaviour (instructions from false ATCO audible for real ATCO)

Event E) False ATCO induced behaviour (instructions from false ATCO not audible for real ATCO)

For each event, the real controller participating in the validation exercise has to decide if this event is induced by a false ATCO or not. Therefore, a detection rate, a detection time and a false alarm rate is calculable.

One additional task of the real controller is to detect unusual trajectories. If such a trajectory is detected, the real controller has to give corrective commands. For this kind of detection, a detection rate, a detection time and a false alarm rate are calculable. Furthermore, the acceptance of the security assistance prototype will be evaluated (including the false alarm and correct detection rate of the prototype, the usefulness of the prototype and the trust in the prototype).

In the baseline, the ATCO will receive no decision support by any system in judging the events. In the solution runs the ATCO will get support by the proposed prototype. The solution will be validated in four separate runs, one run for each detection subsystem of the prototype (speaker verification module; voice pattern anomaly detection module; conformance monitoring module) and one run with the prototype as a complete assistance system (incl. correlation indicator) active. Thereby, the individual benefit of each prototype module can be assessed.

NEXT STEPS AND OUTLOOK

The above described system is aimed at improving the security of ATC communication at a single ATC center. But within the GAMMA platform it is only one component as there also exist other security threats like GNSS spoofing and jamming or satellite communication disruption (referred to as local security systems in Figure 5). The complete system postulated by GAMMA is depicted in Figure 5 where LGSOC means “local GAMMA security operation center”, NGSMP means “national GAMMA security management platform” and EGCC means “European GAMMA control center”. In a next step, some of the components will be combined to support the risk mitigation for coordinated attacks to the ATM system. In a

final step all GAMMA components will be combined and connected by a security management platform, which will collect all available information from the different components and provide national and/or international authorities with assistance in decision making about countermeasures.

In aviation, reaction time to an incident is crucial and normally very short. Concerning safety critical incidents, two main components can be differentiated:

- The detection of a potential dangerous situation
- The elimination of this situation with countermeasures (mitigation)

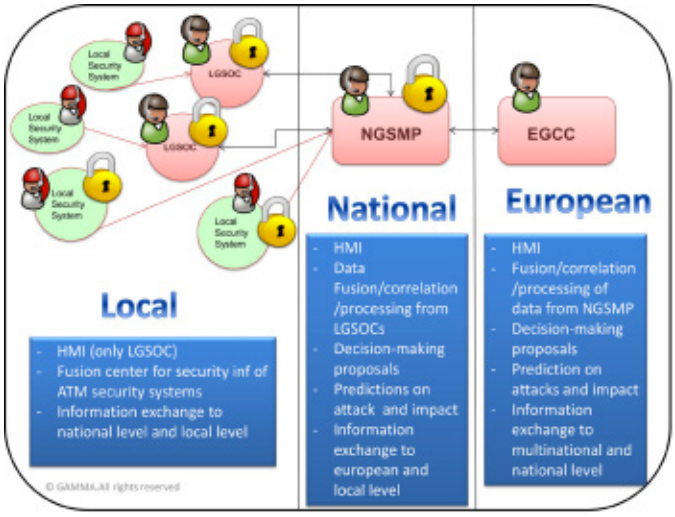


Figure 5: Overall GAMMA solution [16].

Although GAMMA provides also mitigation measures, the main focus lies on detection. A fast and reliable detection of the threats is essential. Therefore, the modules of ATC communication component will run through a continuous improvement process based on the above described validation procedures. Especially the conformance module has a high potential to improve the awareness of unsecure situations. Nevertheless, further research in situational and location dependent typical aircraft behavior and its implementation is required to make conformance monitoring assessment and controller assistance reliable. Considering the second component (mitigation), secure ATC air-ground communication and other security prototypes result in faster detections of security threats. This, in turn, offers more opportunities to mitigate those situations due to more options for actions and/or earlier start of countermeasures. Besides, information gathered by one security prototype can be transmitted to other prototypes and ATM actors in order to increase the awareness concerning possible distributed attacks. Ultimately this may prevent attacks. Eventually the reaction to the detected threat is often depending on national legislation and sovereign power. Fast reaction (especially cross border) needs additional international cooperation, which is far beyond the focus of the GAMMA project. Although measures might be confidential, further international research in this area is strongly encouraged to reduce the security threats of the future.

REFERENCES

[1] Iasiello, Emilio. "Getting Ahead of the Threat: Aviation and Cyber Security." AEROSPACE AMERICA 51.7 (2013): 22-25.

[2] Prinz, J., M. Sajatovic, and B. Haindl. "S/sup 2/EV-Safety and Security Enhanced ATC Voice System." Aerospace Conference, 2005 IEEE. IEEE, 2005.

[3] Eurocontrol, VHF Security Study, Final Report, available: www.icao.int/safety/acp/Inactive%20working%20groups%20library/ACP-WG-N-SWG4-1/sgn04-01-misc01.doc

[4] LiveATC. (2011). 25-MAY-2011 Fake ATC in Action (LTBA-ISTANBUL). Available: http://www.liveatc.net/forums/atcaviation-audio-clips/25-may-2011-fake-atc-in-action-%28ltba-istanbul%29

[5] Chivers, H., J. Hird. (2013, September). “Security Blind Spots in the ATM Safety Culture”. Presented at 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany

[6] EUROCONTROL ATM Security Risk Management Toolkit, ATM Security Risk Assessment Methodology, EUROCONTROL, Edition 1.0, May 2008.

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

[8] Communication Procedures including those with PANS status, ICAO Annex 10, Vol. 2, 6th Edition, July 2001.

[9] Communication Systems, ICAO Annex 10, Vol. III, 2nd Edition, July 2007.

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

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

[12] SESAR ATM Security Risk Assessment Methodology, SESAR Project 16.02.03, D02, Edition 00.01.01, January 2012.

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

[14] D2.3 - Risk Treatment Report, GAMMA Project, D2.3, Final Version, January 2015.

[15] D2.1 – Threat Analysis and Evaluation Report, GAMMA Project, D2.1, Final Version, January 2015.

[16] D4.1 – ATM Security Requirements, GAMMA Project, D4.1, Final Version, March 2015.

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

EMAIL ADDRESSES

Tim H. Stelkens-Kobsch: tim.stelkens-kobsch@dlr.de

Dr. Andreas Hasselberg: Andreas.hasselberg@dlr.de

Dr. Thorsten Mühlhausen: thorsten.muehlhausen@dlr.de

Dr. Nils Carstengerdes: nils.carstengerdes@dlr.de

Michael Finke: michael.finke@dlr.de

Constantijn Neeteson: Constantijn.neeteson@dlr.de

ACKNOWLEDGEMENTS

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.

34th Digital Avionics Systems Conference

September 13-17, 2015

Information Security System (ISS) – Prototype description and capabilities

***Antonio Potenza**, Leonardo*

The Information Security System (ISS) provides a solution to protect data communication at the Airport and for PENS in ATN communication systems that are using new datalink communication services with 4D capabilities (CPDLC and ADS-C) such as AeroMACS and VoIP ATN communication services for the Ground -Ground PENS segment.

The ISS prototype is the Leonardo response to the security assessment carried out at the start of the GAMMA project which highlighted the need to introduce a range of additional security controls:

- The uses of AeroMACS Network End point Authentication/Authorization/Accounting mechanisms to increase the network security of End point systems and applications in the Airport site;

- Increase the security for A/G DL communications for the operation on the Airport site;

- Security mechanisms to detect and to mitigate security threats.

The ISS prototype therefore includes solutions for communication and service authentication that demonstrate the capability of threat mitigation for the vulnerabilities identified during the assessment phase of GAMMA, guaranteeing the required level of confidentiality, integrity and availability.

ISS PROTOTYPE SYSTEM COMPONENTS

The ISS prototype includes the following system components:

- The AeroMACS Networks in the Airport site;

- A/G DL applications for A/C management of ATS procedures;

- EUROCAE Ground VoIP communication;

- ISS Local Network Management System (NMS);

- ISS IPS (Intrusion Prevention System).

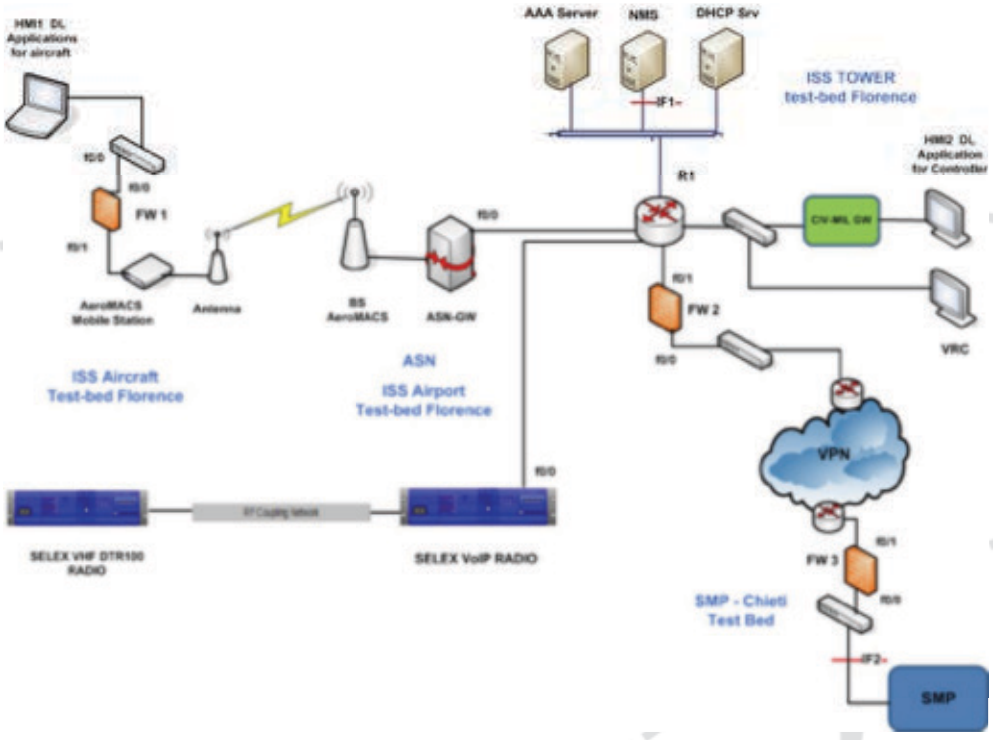


Figure 1: ISS test bed configuration

More specifically the AeroMACS Networks in the Airport site includes the following elements:

AeroMACS Base Station (BS)

The AeroMACS Base Station (BS) is a logical entity complying with the AeroMACS specifications that host one or more access functions. The BS AeroMACS is responsible to receive, amplify and retransmit signals from the airborne mobile station (MS). The main task of a Base Station is to provide radio coverage over the airport area to the airborne subscriber.

AeroMACS Mobile Station (MS)

The AeroMACS Mobile Station (MS) provides connectivity between the aircraft and a base station (BS).

AeroMACS Access Service Network GW

The AeroMACS ASN-GW assists mobility, security data control and handles the IP forwarding. The GW data plane feature includes the mapping of the radio bearer to the IP network, packet inspection, tunneling, admission control, policing, QoS and data forwarding capability.

AAA Server/Proxy

The AAA proxy or server provides policy and Admission Control based on user subscription profiles. The AAA server functionalities set include authorization, authentication, accounting (AAA), context management, profile management and service flow authorization.

ISS – Nework Management System (NMS)

The ISS Network Management System (NMS) oversees AeroMACS networking environments to guarantee high availability of monitoring ISS network elements to avoid degraded service.

The NMS functionalities include network configuration and monitoring, fault management, communication management and reporting problems.

AeroMACS AIR INTERFACE ENCRYPTION FUNCTIONALITIES

The Air interface encryption functionalities provided by the ISS AeroMACS prototype guarantee the adequate level of confidentiality and integrity of A/G communications. These AeroMACS functions involve the BS, MS and AAA AeroMACS network components. The messages between these components are exchanged to enable the End to End encrypted communications:

- The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with MS.
- The BS relays the EAP Request/ Identity to the MS and the MS responds with an EAP Response/ Identity message providing Identity.
- The Authenticator (AAA server) analyses the Identity provided by the MS (Mobile Station). Depending on the domain the MS could be locally authenticated in cases where the MS is in its Home Network.

These main process and protocols between the AeroMACS components are exchanged to enable the End to End encrypted communications:

- The EAP authentication process (tunnelling EAP authentication method) is performed between the MS and the Authentication server via the Authenticator in ASN/ASN-GW. BS provides “relay” of EAP payload from PKMv2 EAP-Transfer messages to Authentication Relay EAP Transfer and vice versa. The Authenticator in ASN/ASN-GW acts in pass through mode and forwards the EAP messages received as a payload from the BS in EAP Authentication request messages to the AAA server using RADIUS Access-Request messages and vice versa.
- PKMv2 3-way handshake (SA-TEK-Challenge/ Request/Response exchange) is conducted between BS and MS to verify the Authorization Key (AK) to be used and to establish the Security Association(s) pre-provisioned for the MS.

ISS A/G CPDLC AND ADS-C COMMUNICATIONS OVER AEROMACS DATALINK AT THE AIRPORT SITE

The A/G CPDLC and ADS-C communications on the ISS prototype includes these main elements that allow aircraft traffic management in the airport for aircraft take-off procedures.

ISS HMI application for Aircraft

HMI Client Application for i4D A/G Data link communication (CPDLC and ADS-C) is an application that simulates pseudo cockpit messages and services over AeroMACS channel communication.

ISS HMI application for Controller

HMI Client Application for i4D A/G Datalink communication (CPDLC and ADS-C) is an application that simulates pseudo working position messages and services over the AeroMACS channel communication.

I4D messages for A/G datalink communications

This paragraph includes a list of CPDLC and ADS-C messages that are exchanged between the pilot HMI and the controller HMI. The ISS prototype includes the following Air Traffic Services (ATS) at the airport’s surface:

- DLIC (DataLink Initiation);
- ACM (ATC Communication Management)
- CRD (Clearance Request and Delivery)

- AMC (ATC Microphone Check)

- 4D-TRAD (4-Dimensional Trajectory Data Link)

The ATS messages are exchanged over the AeroMACS communication channel that includes E2E air encryption mechanisms that guarantee authentication, integrity and data confidentiality.

ISS SECURITY MECHANISMS TO DETECT AND TO MITIGATE SECURITY THREATS

The ISS probe module unit examines network traffic and performs traffic analysis. The DoS policies use traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses. This information offers suggestions on how the Security Network Manager secures the ISS network against specific threat contents.

The IPS functionalities allow executing these main activities:

- Threats monitoring;
- Policy configurations
- Security event reporting

During the network security attacks, the network manager receives data and events related to the security events detected. The ISS sends the security messages to the ISS NMS (Network Management System) and the ISS IPS (Intrusion Prevention System).

The ISS NMS HMI captures and shows the security events “IPS anomaly” detected” (see Figure 2 and Figure 3).

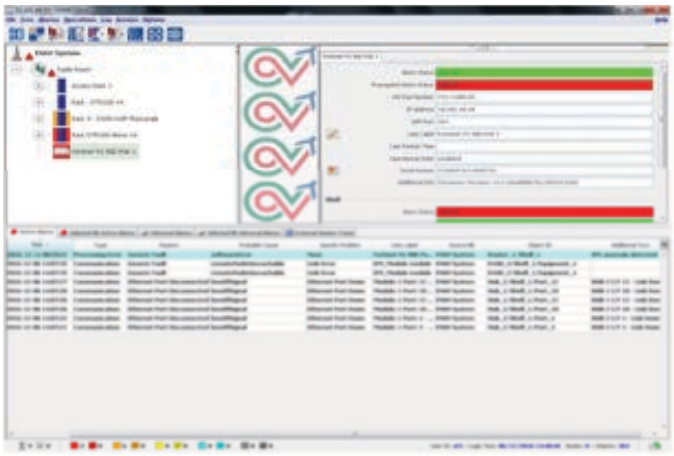


Figure 2: ISS NMS threats event

The Local Network Manager receives the alert of “Anomaly event” and is able to verify the active threats in collaboration with the Security Network Manager.

Figure 3: ISS NMS anomaly event detail

The ISS security events are visible by the Security Network Manager on the ISS IPS HMI (Figure 4) and ISS IPS report (Figure 5).

Figure 4: IPS Security events monitoring

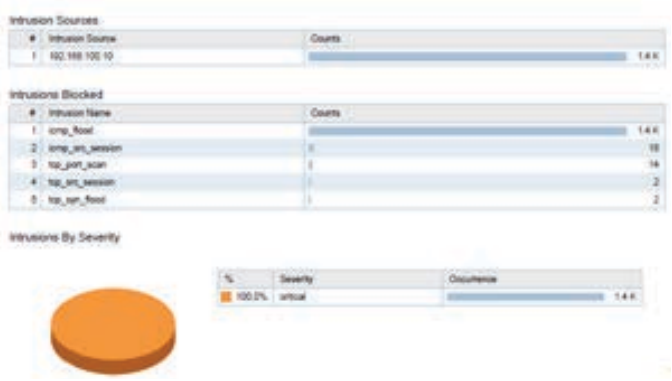


Figure 5 - ISS IPS report

The ISS IPS has the capability to configure an appropriate policy to manage by default the threat scenarios; these policies stored on the IPS can be changed or selected at run time by the Local ISS network Manager to face specific threats or to apply a specify security policy. The figure below provides a screenshot of the ISS policy configuration.

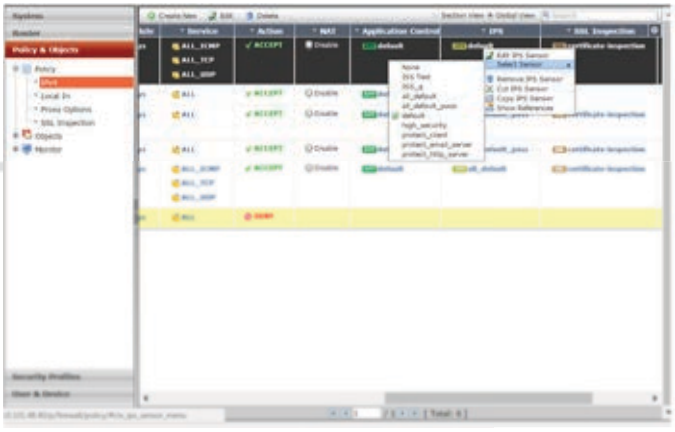


Figure 6 - ISS IPS policy configuration

The ISS IPS allows also to configure new policies with predefined “threshold values” that are used by the “Network Security Manager” to mitigate and prevent possible attacks.

The ISS solution includes the appropriate integration with the Security Management Platform (SMP) prototype to identify and monitor suspect activities and activates the

required countermeasures to minimize or avoid the side attack effect on the communication and ATN service.

The ISS prototype should be seen as part of a broader vision for enlarging the scope for cooperative management by providing situational awareness over the diverse systems which form the ATM system of system.

For this purpose the ISS prototype is able to configure and update security policy configuration, shared with the SMP at National and European level (i.e. security threats details and countermeasures), which enables prevention and mitigates distributed security attacks that could impact on the ATM system and operation.

ISS PROTOTYPE AND STANDARD REFERENCES

- ICAO ATN-OSI 9880 and ATN-IPS 9896 standards;

- EUROCAE ED AeroMACS communication;

- EUROCAE VoIP Standards - ED-136, ED-137 and ED 138 normative;

- PKI recommendation from ICAO WG-I and WG-S.

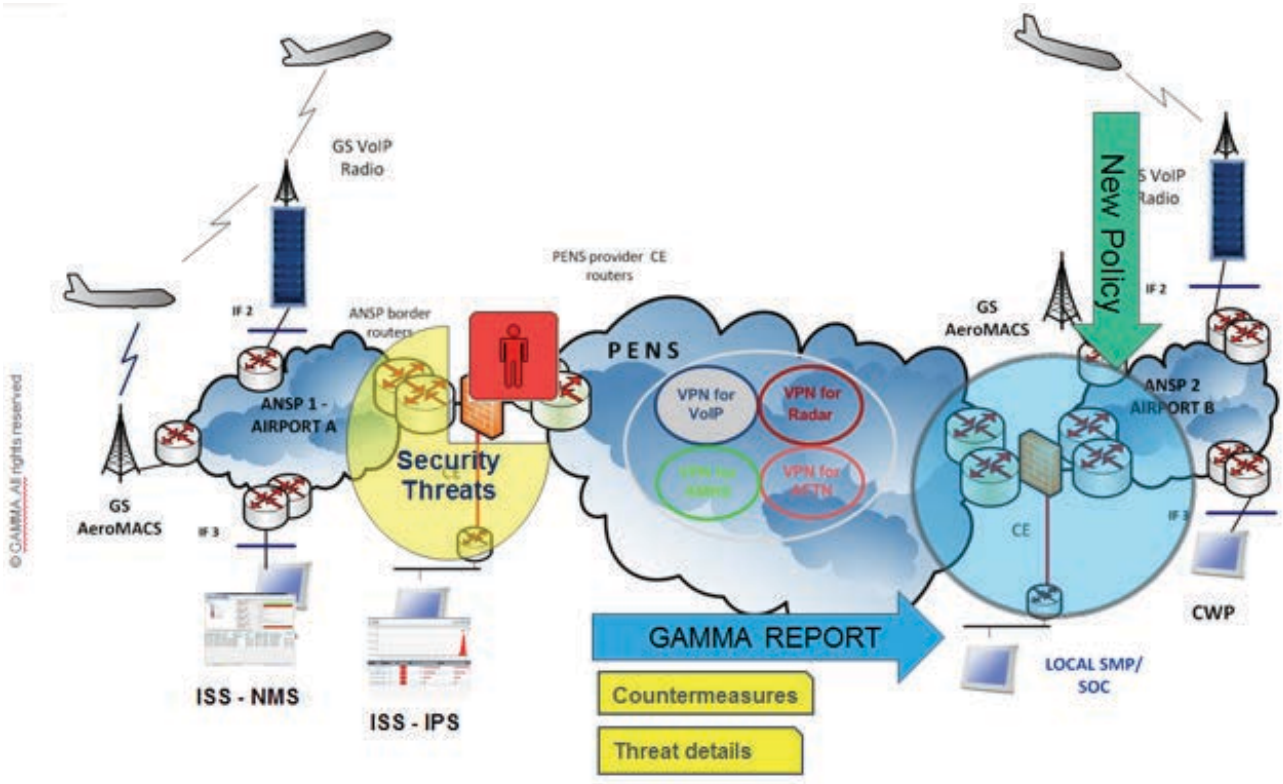


Figure 7 – Security countermeasures and Policy update

Integrated Modular Communication in the Context of GAMMA

***Prof. Hamid Asgari**, Thales UK Limited, Research & Technology*

Commercial aircraft have a communication architecture of diverse radios, routers, switches and associated control equipment with a separate radio generally dedicated to each service. Integrated Modular Communication (IMC) is viewed as an important part of the future Air Traffic Management (ATM) infrastructure. It is an on-board platform to provide secure and reliable aircraft communications for a diverse set of applications. The IMC concept seeks to achieve significant savings in size, weight, power, and cost, for future aeronautical radio fits, by moving away from the existing federated architecture towards an integrated, modular architecture. Combining various systems (i.e., cockpit and cabin) on the same infrastructure as well as integrating the many communication links, could potentially open up the ATM system, thereby increasing vulnerabilities and making the system more prone to security attacks. Therefore, the IMC vision is to achieve secure and reliable communications between the aircraft and the ground over a set of heterogeneous radio links for a diverse set of on-board applications, carried within multiple safety/security domains. Integrating communication links and combining diverse applications in a single platform (IMC) do come with some risks to the ATM communications that could increase the vulnerabilities and the overall risk on launching more attacks, unless adequate security measures are taken.

Work was carried out on the specific functions of IMC under EU FP7 project SANDRA, Innovate UK project SINCBAC, and the UK Aerospace Growth Partnership (AGP) project HARNet. In the GAMMA (Global ATM Security Management) project, we have been specifically looking at the security aspects of IMC. For safety and security of the aircraft and its operations, all possible threats to the aircraft communication systems and its operations must be identified, potential risks must be evaluated, and mitigations must be put in place through efficient implementation of security mechanisms. These security mechanisms must implement and provide different security features to ensure that the IMC system meets the security requirements.

The three main security requirements specified for consideration in information systems are: to prevent unauthorised information disclosure (Confidentiality) and improper malicious modifications of information (Integrity), while ensuring access for authorised entities (Availability). There are several types of attacks on network communications including: disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the storage, tables or packets.

In GAMMA, we have not been focusing on the engineering details of IMC functions (security or otherwise), but as a first step on research into how an IMC can be protected and would integrate in such an overall ATM security management system. That is, we are not proposing a detailed security architecture or in-depth functions for IMC that we expect to be used in a real development environment; any analysis of security requirements and solutions performed in GAMMA can be used but would need to be revisited.

In GAMMA, we have been studying the security risks relevant to IMC operation. We applied Security Risk Assessment Methodology (SecRAM) to IMC for identifying runtime threats, assessing the risks, and defining measures to mitigate them. Specific mitigation measures as IMC's security controls have been proposed to provide cyber resiliency for the IMC. The IMC security controls will be validated in an emulated testbed environment in the GAMMA project.

THE IMC'S FUNCTIONAL PLATFORM

IMC is viewed as an integrated standalone on-board processing platform offering multi-radio off-board communication to/from different stakeholders/providers and on-board network connectivity for cockpit and on-board passenger applications. The IMC consists of the following main sub-systems:

• Router Sub-system (**RoS**) – Responsible for routing traffic between on-board applications and Processors;

• Radio Sub-system (**RaS**) – Responsible for converting application data into a link level format, and routing this to one or more transceivers; It comprises a number of Software Defined Radio entities and includes a number of radio baseband processors together with associated RF transceiver hardware which perform the necessary signal processing needed for the supported bearers.

• Control & Management Subsystem (**CMS**) – Responsible for managing the overall network and security functions, configuring and monitoring of the IMC.

These sub-systems are connected via communication buses. The Packet Buses provide the IP base-band packet interconnect between the IMC subsystems, and between the RoS and the aircraft networks. The IMC off-board communication is via radio links to ground stations. Aircraft on-board applications (i.e., Safety Critical, Cockpit, and Cabin applications) connect to the IMC via the Packet Bus. On-board applications utilising off-board communications services are connected to IMC, via the aircraft networks. The aircraft networks support applications of differing safety criticality levels.

In analysing the security risks, we only considered run-time attacks in GAMMA in order to make provision for built-in countermeasures.

THE IMC ASSETS

The main primary assets, the intangible targets of an attack for IMC in an ATM environment, are shown in Table 1.

Table 1: Primary Assets.

Primary Asset and its Type	*Description*
Air Traffic Communication (Com.) Service as a *Service*	The service that allows the transfer of essential data between ATM systems and an IMC for safety-related purposes, requiring high integrity and rapid response; flight control information, alerting, collision avoidance, etc. The service is used by Safety Critical applica-tions.
Aeronautical Control & Opera-tional commu-nications; as a *Service*	The data service for use by aircraft operators requir-ing high integrity for handling the operation and effi-ciency of flights, and support of passengers; The ser-vice is used by Cockpit applications.
Computing resources; as a *Service*	This refers to the IMC system's internal resources, con-figurations, and operations, e.g. processes, func-tions, and data-bases.
Control and Management data; as *Information*	Any data that is exchanged concerning the operation and management of the IMC system or its connected networks; Exchanged with the Supervisor Control pro-cesses and the external GAMMA Security Man-agement Platform.
Airline data; as *Information*	Any data that is exchanged to or from airliner's do-main i.e., the operational and airline administrative informa-tion to both Cockpit and Cabin applications.
User data; as *Information*	Any data that is transferred to or from a Cabin appli-ca-tion process. This is done by a passenger device, acces-sing the aircraft network (e.g., WiFi or telecom services).

Supporting Assets (SA) are tangible entities that enable and support the existence of primary assets. Table 2 lists, and briefly explains, the supporting assets that may be targeted by a threat scenario and their related primary assets.

Table 2: Supporting Assets.

Supporting Asset	*Description*	*Primary Asset*
IMC system	Integrated Modular Communica-tion as a complete system in the ATM environment	Computing resources; Com. Service; Airline, User, or C&M data
IMC's RoS	Routes data traffic from on-board applications to RaS or vice versa.	Computing resources, Airli-ne, User, or C&M data
IMC's RaS	Converting data into a link level format, passing data to one or more transceivers	Computing resources, Airli-ne, User, or C&M data
IMC's CMS	The entity performing the overall management of IMC functions and security	C&M data
IMC's Inter-nal BUS	IMC internal packet bus as the data link between RoS, RaS, and CMS	Airline, User, or C&M data
Satellite link	Satellite link to provide world-wide reliable com. channels	Com. Service, Airline, User, or C&M data
HF/UHF/ VHF links	Different radio Data links	Com. Service, Airline, User, or C&M data
Wireless access inks	Broadband wireless access sys-tems for on-the-ground com.	Airline, User, or C&M data
Cellular link	Provides cellular connectivity such as 3G.	User data

THREAT SCENARIOS AND RISK ASSEMMENT

We mainly focused on intentional threats to the IMC network and its assets. These threats are intended for confidentiality, integrity and availability violation, disruption of services, unauthorised access to data and objects, and unauthorised disclosure of information.

Table 3 shows the identified IMC threats. For more details about these threats please see GAMMA deliverable D2.1.

For each threat, the impact is valued and assessed according to the loss or degradation of confidentiality, integrity, and availability for every primary asset. The likelihood is built from a split into 'frequency of occurrence' of the threat source and 'potentiality' that, once the threat source occurs, the threat scenario

sequence is completed successfully. The impact and likelihood scoring are subjective and depends on definition of scales defined in SecRAM, best practices, intuition, and the security experts' knowledge. Once the likelihood and impact of each threat has been assessed, the risk-level has been calculated using the SecRAM Guidance document.

Table 3: Identified IMC Threats.

Description of Threats
Threat 1: On-board application attack: An application on board the aircraft uses its data connection to the IMC to attack an ATM primary asset (e.g. flight/airline information managed by another application).
Threat 2: Off-board application attack: An off-board application uses its data connection to the IMC to attack an ATM primary asset. This could be a ground segment application, or something external to the ATM system (e.g., Internet traffic destined for the cabin).
Threat 3: Subverted software or hardware: Corrupted software or hardware in the IMC attacks an ATM primary asset (e.g., denying communication to ATC).
Threat 4: Abuse of management interface: An administrator of the IMC (e.g. someone setting configuration parameters) abuses his/her privileges, or someone impersonates the administrator, and uses this to attack an ATM primary asset.
Threat 5: Jamming of data links: A jamming device is used in prox-imity to ATM channels to perform this attack. These devices prevent IMC from communicating application data.

SECURITY CONTROLS

The treatment actions or security controls are defined to protect supporting assets. The risk treatment option that has been selected is the "Reduce" action to combat threats with 'Medium' and 'High' risk levels. Once the type of treatment has been evaluated, the best set of security controls must be chosen. The security controls are iteratively identified, firstly through the application of MSSCs developed by SESAR 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 security controls or through refinement of the MSSCs. In summary, the security controls specified for IMC can be categorised as below:

- Authenticating users of the IMC.
- Controlling access to the resources via access control mechanisms.
- Using cryptographic protection to protect the confidentiality and integrity of assets. This requires the services of a Key Manager.
- Monitor and control the relevant processes in the IMC; The risks can be reduced by performing monitoring of activities to identify activities that are not expected and then take actions against them.

More details about these specified security controls are given in GAMMA deliverable D2.3.

In conclusion, the general aim of GAMMA is to validate, verify and demonstrate the security related capabilities introduced in the project (including those of the IMC) for future ATM context. We performed a study to identify and prioritise run-time threats to the IMC. Using SecRAM methodology step-by-step, we identified possible threats to IMC, assessed the risk levels related to these threats, and identified the security controls to bring the high risk levels down. Work is being conducted in the GAMMA project to implement an emulated IMC for verifying and validating the defined security controls.

Security Risk Assessment and Risk Treatment for Integrated Modular Communication

***Hamid Asgari**, Senior Member IEEE, **Sarah Haines**, and **Adrian Waller**, Thales UK Limited, Research & Technology, Worton Drive, Worton Grange Business Park, Reading RG2 0SB, United Kingdom*

ABSTRACT

Integrated Modular Communication (IMC) is an on-board platform to provide secure and reliable aircraft communications for a diverse set of applications. IMC is viewed as an important part of the future Air Traffic Management (ATM) infrastructure. Integrating communication links and combining diverse applications in a single platform (IMC) do come with some risks to the ATM communications that could potentially increase vulnerabilities and make the system more prone to security attacks. There are several types of attacks on network communications such as disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the information. In this study, the Security Risk Assessment Methodology (SecRAM) is applied to IMC for identifying runtime threats, assessing the risks involved, and defining measures to mitigate them. The risk assessment is performed to evaluate the impact and likelihood of occurrence of attacks relevant to the identified threats and the resulting risk levels. Consequently, specific mitigation measures as IMC's security controls are proposed to provide cyber resiliency for the IMC. The IMC security controls will be validated in an emulated testbed environment in the GAMMA project.

Keywords – ATM, Security, Risk Assessment, Threat, IMC.

I. INTRODUCTION

Commercial aircraft have a communication architecture of diverse radios, routers, switches and associated control equipment with a separate radio generally dedicated to each service. The Integrated Modular Communications (IMC) concept seeks to achieve significant savings in size, weight, power, and cost, for future aeronautical radio fits, by moving away from the existing federated architecture towards an integrated, modular architecture. Combining various systems (i.e., cockpit and cabin) on the same infrastructure as well as integrating the many communication links, could potentially open up the ATM (Air Traffic Management) system to more attacks, thereby increasing vulnerabilities and the overall risk, unless adequate security measures are taken. Therefore, the IMC vision is to achieve secure and reliable communications between the aircraft and the ground over a set of heterogeneous radio links for a diverse set of on-board applications, carried within multiple safety/security domains.

Works has been carried out on the specific functions of IMC under EU FP7 project of SANDRA [1], Innovate UK project of SINCBAC [2], and the UK Aerospace Growth Partnership (AGP) project of HARNet [3]. In the GAMMA (Global ATM Security Management) project [4], we have been looking at the security aspects of IMC. For safety and security of the aircraft and its operations, all possible threats to the aircraft communication systems and its operations must be identified, potential risks must be evaluated, and mitigations must be put in place through efficient implementation of security mechanisms. These security mechanisms must implement and provide different security features to ensure that the IMC system meets the security requirements.

The three main security requirements specified for consideration in information systems are: to prevent unauthorised information disclosure (Confidentiality) and improper malicious modifications of information (Integrity), while ensuring access for authorised entities (Availability). There are several types of attacks on network communications including: disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the storage, tables or packets.

GAMMA is complimentary to SESAR (Single European SKY ATM Research) project [5] by developing security solutions for current and next generation ATM which is being defined by SESAR. In the GAMMA project, we have been focusing on the methodologies used for: 1) risk assessment and selection of security controls/functions 2) producing operational and system architectures of ATM security systems including IMC. These architectures are described by the enterprise architecture views of the NATO Architecture Framework (NAF) [6]. GAMMA and SESAR both use the NAF and adopt the same modelling tool (MEGA) [7], opening the way for the GAMMA architecture outputs to be reusable in SESAR. GAMMA has also adopted the methodologies developed by SESAR in WP16 including SecRAM (Security Risk Assessment Methodology) [8] and MSSC (Minimum Set of Security

Controls) [9].

We have not been focusing on engineering details of IMC functions (security or otherwise), but on research into how an IMC can be protected and would integrate in such an overall ATM security management system. That is, we are not proposing a detailed security architecture or in-depth functions for IMC that we expect to be used in a real development environment; any analysis of security requirements and solutions performed in GAMMA can be used but would need to be revisited.

A significant body of works exists in the literature on risk management. Among these works, there are established security risk assessment standards, frameworks, methodology and guides (e.g., ISO/IEC 31010 [10], NIST SP800-30 [11], MITRE [12], and ENISA [13]) that are used to aid formal risk analysis procedures in various contexts. The SESAR SWP16.2 defined a methodology, called SecRAM [8]. SecRAM is applied to ATM contexts. An example of its application is given in [14] by building a relevant threat scenario and designing a risk treatment for a cloud-based ATM environment.

In this paper, we report on the use of the SecRAM methodology for identifying threats and assessing the associated risks for IMC. Accordingly, we establish the context and set out the scope for the security analysis of IMC, assessing the risk levels, and set the scene for validating the identified security controls. For validation purposes, the defined security enablers/controls are checked against the stakeholders' security requirements and needs in order to meet them. Embedding security controls in the IMC architecture for combating run-time threats is a step towards the security-by-design concept enabling cyber resiliency and avoiding incremental updates and plug-ins. Cyber resiliency enablement allows the networked systems to be resilient against persistent, stealthy attacks targeted at cyber assets [15].

The remainder of this paper is structured as follows. After this brief introduction in Section I, Section II describes the risk assessment methodology. Section III briefly explains the IMC functional architecture as the context for this security analysis, the scope of the risk assessment study and the assets. Section IV specifies the threat scenarios relevant to the IMC. The security risk assessment process is described in Section V. Section VI proposes the security controls to put in place to mitigate the threats with high risk levels. The validation process is briefly discussed in Section VII. Section VIII concludes the paper and discusses the further work plan.

II. RISK ASSESSMENT METHODOLOGY

The evaluation of the threats proposed here will follow the SecRAM methodology [8]. SecRAM is the ISO 27005 based Risk Assessment methodology [16] developed by the SESAR program. This methodology requires establishing the context for defining the boundaries of what one wants to analyse; sets out the scope of the security analysis; and specifies the criteria that will be used to assess the risk, in order to provide consistent and defensible results.

The security risk assessment process adheres to the following steps:

1. Establish the context and an accurate scope: description of the system, boundaries, and the dependencies on other systems;

2. Identify the assets that have value for the achievement of stakeholders' objectives;

3. Identify the threats and threat scenarios that an attacker may use to access an asset;

4. Evaluate the impact of attacks, assessing the harm resulting from an attack in terms of Confidentiality, Integrity, and Availability (CIA);

5. Evaluate the likelihood of each threat scenario that could occur;

6. Assess the security risk level associated to the threats based on their likelihood and impact on the assets;

7. Evaluate and verify the evaluated risk level against the defined security objectives. Security objectives correspond to the level of risk that a primary asset is prepared to accept on CIA, before any action is necessary to reduce it;

8. Risk treatment by defining the action to accept, tolerate, reduce, avoid, or transfer the risk; If the action is to reduce the risk, define a set of security controls and the associated requirements to reduce the risk to an acceptable level (i.e. within the risk appetite, see [8]);

9. Risk treatment by defining appropriate action to manage the risk as below:

- Accept or tolerate, which means the risk level is low enough, no further action is needed.

- Reduce or treat, which means the risk must be reduced to an acceptable level (i.e. within the risk appetite) by defining a set of security controls and the associated requirements.

- Avoid or terminate, which means that the risk is too high and treating it is too costly, a decision may be made to withdraw the activity or change its nature so that the risk is not present anymore.

- Transfer, which means the risk should be transferred to another party who can most effectively manage the particular risk.

10. Implementation of security controls identified above.

We now apply the above process to the IMC architecture.

III. CONTEXT, SCOPE, AND ASSETS

A. The Context – IMC

IMC is viewed as an integrated standalone on-board processing platform offering multi-radio off-board communication to/from different stakeholders/providers and on-board network connectivity for cockpit and on-board passenger applications. The functional architecture of the IMC is shown in Figure 1. The IMC consists of following main sub-systems:

- Router Sub-system (RoS) – Responsible for routing traffic between on-board applications and Processors;
- Radio Sub-system (RaS) – Responsible for converting application data into a link level format, and routing this to one or more transceivers; It comprises a number of Software Defined Radio entities and includes a number of radio baseband processors together with associated RF transceiver hardware which perform the necessary signal processing needed for the supported bearers.
- Control & Management Subsystem (CMS) – Responsible for managing the overall network and security functions, configuring and monitoring of the IMC.

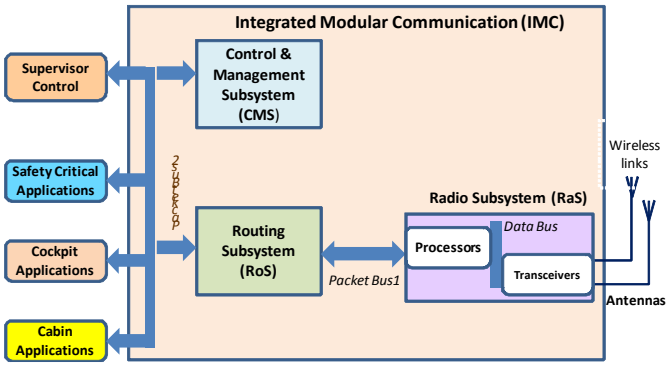


Figure 1: The functional architecture of Integrated Modular Communication and associated applications.

These sub-systems are connected via communication buses. The Packet Buses as shown in Figure 1 provide the IP base-band packet interconnect between the IMC subsystems, and between the RoS and the aircraft networks. The IMC off-board communication is via radio links to ground stations. Aircraft on-board applications (i.e., Safety Critical, Cockpit, and Cabin applications) connect to the IMC via the Packet Bus2. On-board applications utilising off-board communications services are connected to IMC, via the aircraft networks. The aircraft networks support applications of differing safety criticality levels.

B. Scope

Establishing the context means defining the bounds of what you want to analyse. Design time identification of vulnerabilities in the specification of protocols and functions and mitigation of these are out of the scope of this paper. We only consider run-time attacks in order to make provision for built-in countermeasures.

C. Asset Identification

There are two types of assets: primary and supporting. Primary Assets (PA) are the intangible targets of an attack, which are valuable to an IMC network and its stakeholders. There are two main types of primary assets: information and services. A successful attack would result in damage to the primary assets and have an impact on the network operation.

The main primary assets for IMC in an ATM environment are shown in Table 1.

Table 1: Primary Assets.

Primary Asset	*Type*	*Description*
Air Traffic Communication (Com.) Service	Service	The service that allows the transfer of essential data between ATM systems and an IMC for safety-related purposes, requiring high integrity and rapid response; flight control information, alerting, collision avoidance, etc. The service is used by Safety Critical ap-plications.
Aeronautical Control & Operational communcations	Service	The data service for use by aircraft operators requiring high integrity for handling the operation and efficiency of flights, and support of passengers; The service is used by Cockpit applications.
Computing resources	Service	This refers to the IMC system's internal resources, configurations, and operations, e.g. processes, functions, and databases.
Control and Management data	Information	Any data that is exchanged concerning the operation and management of the IMC system or its connected networks; Exchanged with the Supervisor Control processes and the external GAMMA Security Management Platform.
Airline data	Information	Any data that is exchanged to or from airliner's domain i.e., the operational and airline administrative information to both Cockpit and Cabin applications.
User data	Information	Any data that is transferred to or from a Cabin application process. This is done by a passenger device, accessing the aircraft network (e.g., WiFi or telecom services).

Supporting Assets (SA) are tangible entities that enable and support the existence of primary assets. Entities involved in storing, processing and/or transmitting primary assets are classified as supporting assets. They may have vulnerabilities that can be exploited by threats targeting the primary assets. Table 2 lists, and briefly explains, the supporting assets that may be targeted by a threat scenario and their related primary assets.

Table 2: Supporting Assets.

Supporting Asset	*Description*	*Primary Asset*
IMC system	Integrated Modular Commu-nication as a complete sys-tem in the ATM environment	Com. Service Comput-ing resources, Airline data, User data, C&M data
IMC's Routing Sub-system (RoS)	Routes data traffic from on-board applications/processes to radio sub-system and vice versa.	Computing resources, Airline data, User data, C&M data
IMC's Radio Sub-system (RaS)	Converting data into a link level format, passing data to one or more transceivers	Computing resources, Airline data, User data, C&M data
IMC's Control & Management Sub-system (CMS)	The entity performing the overall management of IMC functions and security	C&M data
IMC's Internal BUS	IMC internal packet bus as the data link between RoS, RaS, and CMS	Airline data, User data, C&M data,
Satellite link	Satellite link to provide worldwide reliable commu-nication channels	Com. Service, Airline data, User data, C&M data
HF/UHF/VHF links	Different radio Data links	Com. Service, Airline data, User data, C&M data,
Wireless access inks	Broadband wireless access systems for on-the-ground communication.	Airline data, User data, C&M data
Cellular link	Provides cellular connectivi-ty such as 3G.	User data

IV. THREAT SCENARIOS

In this paper, we mainly focus on intentional threats to an IMC network and its assets. Therefore, we do not analyse the complete spectrum of threats (e.g. faults, accidental, natural, terrorist damages, or unintentional misconfiguration of policies). Only the most relevant threats have been selected and applied to the supporting assets. These threats are intended for confidentiality, integrity and availability violation, disruption of services, unauthorised access to data and objects, and unauthorised disclosure of information.

Table 3 shows the identified IMC threats. Threat 1 (T-IMC1) and Threat 2 (T-IMC2) correspond to attacks from on-board and off-board applications respectively. Threat 3 (T-IMC3) is specified in which an attacker inserts malicious software into the IMC. An example of Threat 3 is related to the configuration of the router that needs to be protected. There are known ways of achieving this protection. Threat 4 (T-IMC4) is related to the abuse of administrator privilege. Threat 5 (T-IMC5) is related to Jamming attacks. For more details please see GAMMA deliverable D2.1 [4].

Table 3: Identified IMC Threats.

IMC Threat	*Description*
T-IMC1	**On-board application attack**: An application on board the aircraft uses its data connection to the IMC to attack an ATM primary asset (e.g. flight/airline information managed by another application).
T-IMC2	**Off-board application attack**: An off-board application uses its data connection to the IMC to attack an ATM pri-mary asset. This could be a ground segment application, or something external to the ATM system (e.g., Internet traf-fic destined for the cabin).
T-IMC3	**Subverted software or hardware**: Corrupted software or hardware in the IMC attacks an ATM primary asset (e.g., denying communication to ATC).
T-IMC4	**Abuse of management interface**: An administrator of the IMC (e.g. someone setting configuration parame-ters) abus-es his/her privileges, or someone imperso-nates the adminis-trator, and uses this to attack an ATM primary asset.
T-IMC5	**Jamming of data links**: A jamming device is used in prox-imity to ATM channels to perform this attack. These devic-es prevent IMC from communicating application data.

The impact on targeted supporting assets of the IMC Threats 1 to 4 will be the leakage or unauthorised modification of data within the IMC, and could cause reduced availability or even complete failure of the IMC.

V. SECURITY RISK ASSESSMENT

For each threat, the impact on the Confidentiality, Integrity and Availability of the information and services is assessed according to the following scale [8]:

- Scale 1: No impact / Not Applicable
- Scale 2: Minor – limited impact to the IMC operation, but it is still able to function
- Scale 3: Severe – performance of an IMC process is compromised in order to malfunction
- Scale 4: Critical – performance of the IMC functions is compromised that can have major consequences
- Scale 5: Catastrophic – The IMC operation and its network are compromised making the IMC system inoperable/malfunction.

The impact is valued and assessed according to the loss or degradation of Confidentiality (C), Integrity (I), and Availability (A) for every primary asset. The overall impact is then calculated as the highest of the three impact values of C, I, and A.

According to the SecRAM, the likelihood is built from a split into 'exposure' or frequency of occurrence of the threat source and 'potentiality' that, once the threat source occurs, the threat scenario sequence is completed successfully. Once both likelihood layers have been

evaluated, the overall likelihood is obtained from the average of both values rounded up to the next integer. Both likelihood layers related to a threat scenario can be estimated and realised according to the scales shown in Table 4.

Table 4: Likelihood scales.

Scale	*Exposure*	*Potentiality*
1	Very rare	Very unlikely - practically impossible
2	Rare	Unlikely – very low chance
3	Occasionally	Likely - possible
4	Frequently	Very likely – high chance in medium term
5	Continuous	Certain - high chance in short term

The impact and likelihood scoring shown in the first column of tables (Tables 4 to 8) is subjective and depends on definition of scales above, best practices, intuition, and the security experts' knowledge. Once the likelihood and impact of each threat has been assessed, the risk-level can be calculated using Table 25 given in the SecRAM Guidance document [17].

VI. SECURITY CONTROLS

As stated in [8], treatment actions or security controls are defined to protect supporting assets. They are a collection of measures for managing risks and to ensure the security objectives are met. They include, but are not limited to, procedures, policies, more robust technical solutions, and management actions. The security objective level comes from the definition of the Impact Area such as performance, economic, etc., see [8]. A security need is defined whether a risk needs to be treated or not; when the level of a risk is higher than the security objective of a supporting asset (i.e. the lowest security objective it is targeting), a treatment shall be applied.

The risk treatment option should be selected from the actions defined in step 8 of Section II (i.e. Tolerate, Reduce, Avoid, or Transfer). Normally, the "Tolerate" option for the threats with 'Low' risk level and the "Reduce" option in combating threats with 'Medium' and 'High' risk levels are selected to meet security objective levels.

In defining the security controls, it is important to take into account the three parameters (i.e., likelihood, impact, and risk-level). For example, if the likelihood is high and impact is low, but risk level is high, the security control should be primarily defined to counter the likelihood and it could overlook the impact. Once the type of treatment has been evaluated, the best set of security controls must be chosen.

In this paper, we only show security controls for threats with a risk-level of high. This is to reduce the risk level to the acceptable level that corresponds to the security objective of supporting assets. The most feared and critical threat scenarios are with the risks evaluated as High with low security objectives. These should have high priority in treating them. The security controls are iteratively identified, firstly through the application of MSSCs developed by SESAR [9] 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 security controls or through refinement of the MSSCs. Table 4 to Table 8 show the results of security assessment for T-IMC1 to T-IMC5 respectively and the relevant MSSCs that must be put in place to reduce the risk level from High to Low. More details about these specified security controls are given in GAMMA deliverable D2.3 [4]. In these tables, the first column shows the Impact, Likelihood, Risk level, and Security Objective. The second column shows the Supporting Asset (SA), the third column shows the relevant C, I, or/and A as security requirement, and the forth column describes the Security controls to protect the SA.

Table 5: Defined Security Controls for threat T-IMC1.

	SA	CIA	MSSC Description for T-IMC1
	IMC	C	Authorise connections to ATM network and to IMC
	CMS	C	Protect ATM system and IMC documentation against unauthorised access
	IMC	CI	Protect messages from unauthorised access and modification
	Internal BUS	CI	Monitor the use of ATM services and IMC
	CMS	CI	Restrict access to the IMC to authorised users only
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	IMC	I	Protect IMC and ATM against malicious code
	CMS	I	Control management process for ATM and IMC to prevent malicious software changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in IMC system or services.
	IMC	A	Test back-up copies of IMC software regularly

Table 6: Defined Security Controls for threat T-IMC2.

	SA	CIA	MSSC Description for T-IMC2
	IMC	C	Authorise connections to ATM network and to IMC
	CMS	C	Protect ATM system and IMC documentation against unauthorised access.
	Internal BUS	CI	Protect information exchange
	Internal BUS, RoS, RaS	CI	Protect messages from unauthorised access and modification
	Internal BUS	CI	Monitor the use of ATM services and IMC

	SA	CIA	MSSC Description for T-IMC2
	IMC	CI	Restrict access to the ATM to authorised users only
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	CMS	I	Protect IMC and ATM against malicious code
	IMC	I	Control management process for ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in ATM systems or services
	IMC	A	Test back-up copies of ATM and IMC software regularly

Table 7: Defined Security Controls for threat T-IMC3.

	SA	CIA	MSSC Description for T-IMC3
	CMS	CI	Secure access controls. ATM and IMC only accessible by authorised personnel
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	CMS	I	Protect IMC and ATM against malicious code
	IMC	I	Control management process for ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in ATM systems or services
	CMS	CI	Secure access controls. ATM and IMC only accessible by authorised personnel

Table 8: Defined Security Controls for threat T-IMC4.

	SA	CIA	MSSC Description for T-IMC4
	CMS	CI	Monitor and record privileged operations
	CMS	C	Users must protect their authentication information or devices.
	CMS	CI	ATM accessible to authorised users only
	CMS	CI	Restrict the use of utility programs that might be capable of overriding system and application controls
	IMC	CI	Users shall ensure that unattended equipment has appropriate protection.
	CMS	I	Protect log files
	IMC	A	Test back-up copies of ATM and IMC software regularly

Table 9: Defined Security Controls for threat T-IMC5.

	SA	CIA	MSSC Description for T-IMC5
See *Note 1*	All IMC's wireless communication links	CIA	Use anti-jamming techniques; it is out of scope of this paper

Note 1: In Table 9, the related parameters are: Impact = 5, Likelihood = 3, Risk Level = High, and the Security Objective = Low.

From the above tables, the threats can be mitigated using existing mechanisms to be considered as built-in security controls/enablers for IMC, to satisfy the stated security requirements (see Figure 2). The GAMMA deliverable D4.3v2 provides more details of functional architecture and interactions of its components for embedding the defined security controls in the fabric of IMC [4].

To summarise, the security controls specified in Tables 4 to 8 can be categorised as below:

- Authenticating users of the IMC.
- Controlling access to the resources via access control mechanisms.
- Using cryptographic protection to protect the confidentiality and integrity of assets. This requires the services of a Key Manager.
- Monitor and control the relevant processes in the IMC.

The risks can be reduced by performing monitoring of activities to identify activities that are not expected and then take actions against them.

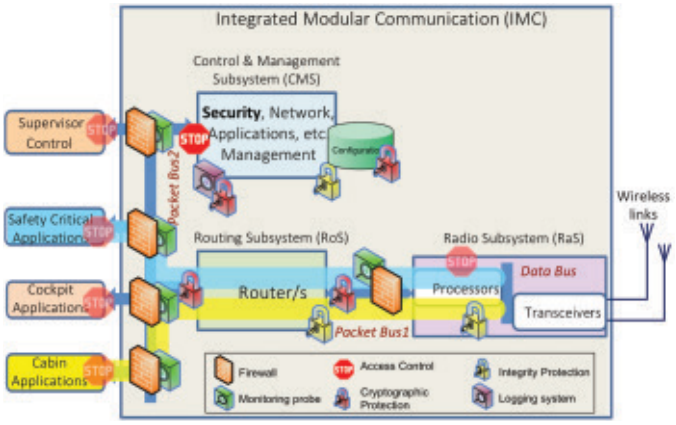


Figure 2: The IMC architecture with security controls.

VII. VALIDATION, VERIFICATION, AND EVALUATION

The general aim of GAMMA is to validate, verify and demonstrate the security related capabilities introduced in the project (including those of the IMC) for future ATM context. Validation is regarded as the process of checking whether the proposed solution satisfies the identified requirements. Verification is the process of checking whether the proposed solution complies with the design specification in order to function correctly as expected. Evaluation is the process of determining that the proposed solution meets the desired quality and performance characteristics. It should be noted that there is always a trade-off between security and performance, as the security mechanisms introduce additional delay in processing and forwarding messages. These three processes are crucial for understanding the implications of applied methods. The overall assessment of the project outcome will be carried out following the European Operational Concept Validation Methodology

(E-OCVM) [18] currently used within SESAR.

The plan for validation exercises and the validation platform are given in GAMMA project deliverables D5.1 and D5.3 respectively [4]. In the final stage of the project, the applicability of the project outcome will be demonstrated and experts' knowledge will be used to validate the effectiveness of security controls in reducing the risks and in satisfying the identified security requirements.

VIII. CONCLUSIONS

In this paper, we described the use of a security risk assessment methodology (SecRAM) and performed a study to identify and prioritise run-time threats to the IMC. Using this methodology step-by-step, we identified possible threats to IMC, assessed the risk levels related to these threats, and identified the security controls to bring the high risk levels down. We established that some of the threat scenarios require monitoring to reduce the threat risk levels. In order to realise the security state of IMC's network system, monitoring should be carried out for observing and gathering data from different indicators, processing events, identifying adversary activities, and possible damages. Work is being conducted in the GAMMA project to implement a number of security-enabled prototypes including an emulated IMC relevant to the ATM context for validation purposes individually and collectively.

REFERENCES

[1] SANDRA project - Seamless Aeronautical Networking through integration of Data links Radios and Antennas, http://sandra.aero/2013/.

[2] SINCBAC Project - Secure Integrated Broadband and ATM Communications, http://gtr.rcuk.ac.uk/projects?ref=101290.

[3] HARNet project - Harmonised Antennas, Radios, and Networks, Innovate UK, http://gtr.rcuk.ac.uk/projects?ref=113029.

[4] GAMMA (Global ATM Security Management), http://www.gamma-project.eu/; Project Deliverables, D2.1: "Treat Analysis and Evaluation Report", Jan. 2015; "D2.3: Risk Treatment Report", Jan. 2015; D4.3: "ATM Solution Architecture model – Version 2", April 2015; D5.1, "Validation Excersies Plan", D5.3: Validation Platform Architecture Definition".

[5] SESAR (Single European Sky ATM Research) collaborative project, SESAR website: http://www.sesarju.eu/.

[6] NATO Architecture Framework (NAF) Version 3.0, Nov. 2007, https://en.wikipedia.org/wiki/NATO_Architecture_Framework,

[7] MEGA (Model Based System Engineering) tool, http://www.mega.com/en/consulting/model-based-system-engineering.

[8] SESAR Joint Undertaking, "SESAR ATM Security Risk Assessment Methodology" – Project 16.02.03 D02, 2013, SESAR website: HTTP://WWW.SESARJU.EU/.

[9] SESAR ATM Project 16.02.05-D137, SESAR Minimum Set of Security Control, SESAR website: HTTP://WWW.SESARJU.EU/.

[10] ISO/IEC 31010: Risk management - Risk assessment techniques, Geneva, International Organization for Standardization & International Electrotechnical Commission, 2009, preview on line: https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en

[11] National Institute of Standards and Technology (NIST), "Guide for Conductig Risk Assessment", Special Publication 800-30 Rev. 1, Sept. 2012, available on line: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[12] The MITRE Institute, "Risk Management", System Engineering Guide, Sept. 2013, available on line: http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management.

[13] European Network and Information Security Agency (ENISA), "Risk Management: Implementation principles And Inventories for Risk Management/Risk Assessment methods and tools", June 2006.

[14] A. Marotta, et al., "Applying the SecRAM Methodology in a Cloud-based ATM Environment", Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg Germany, pp. 807 – 813, Sept. 2013.

[15] D. J. Bodeau, and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement", MITRE Technical Report, May 2013, available on line: http://www.mitre.org/publications/technical-papers/cyber-resiliency-assessment-enabling-architectural-improvement.

[16] Bristish Sandard, "ISO/IEC 27005", 1st edition, chapter 7 (guidance for establishing the context), 2008, available on line: www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf.

[17] SESAR Joint Undertaking, "SESAR ATM SecRAM Implementation Guidance Material", D03, Edition 00.02.06, May 2013, Project 16.02.03, SESAR official website: HTTP://WWW.SESARJU.EU/.

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

EMAIL ADDRESSES

{Hamid.Asgari, Sarah.Haines, Adrian.Waller}@uk.thalesgroup.com

Work towards this paper was partially funded by the Commission of the European Union, FP7 Collaborative GAMMA Project, 312382. The authors would like to thank their project partners in the development of work presented in this paper.

*The paper entitled as "**Security Risk Assessment and Risk Treatment for Integrated Modular Communication**" was published in the proceeding of International conference on Availability, Reliability, and Security (ARES), ATMSec Workshop, held in Salzburg, Austria, Sept. 2016, http://www.ares-conference.eu/ares2016/www.ares-conference.eu/conference/index.html.*

SATCOM Security Prototype

David Perez, *Thales Alenia Space Spain*

INTRODUCTION

At current aeronautics, several risks can be detected in terms of threats, security levels and management of the systems. One of the main issues with the aircrafts is that we are not able to detect them when they are out of the civil radar coverage (without involving military radars) in those circumstances an attack to the aircraft cannot be detected from ground.

The satellite systems have capabilities to cover this lack at the sky, giving to the operator extra functionalities and new information to cover the aircraft when out of the radar coverage. A simple satellite system consist on several parts where the most important to make the communication are the satellite terminals, which send the information to the satellite itself, the link between the satellite and both sides (satellite terminals and ground base station) and the Human Machine Interface (HMI) to display the information from the satellite terminals.

SATCOM CONCEPT

In order to improve the aircraft security when it is out of the civil radar coverage, a SATCOM concept appears on the GAMMA project. The purpose of the SATCOM security prototype is to detect and offer countermeasures as fast as possible to different threats, managing and controlling the SATCOM system involved in ATM in terms of operation, administration and maintenance.

A module of the prototype is placed at the aircraft, using two Satellite Communications are deemed critical for future ATM, hence satellite related threats need to be addressed, such as:

- RF interference that could be generated by known and unknown equipment (either intentional/malicious or unintentional) transmitting in the useful bandwidth.
- Intrusion from terrestrial networks, to which the Satcom system connects.
- Denial of Service attacks from terrestrial networks to which the Satcom system connects.
- Data communication eavesdropping.
- Satellite system signalling spoofing.

With these objectives in mind, the design of the SATCOM security prototype relies on the coordinated work of a set of functional modules integrated in a client-server software architecture, where each module will be responsible of a set of security functions. Each module will have a server side and a client side. The server side has two major responsibilities: to offer services to client layer, so the client layer does not need to obtain information from another site; and to serve as an integrator for external systems.

The way of working or the flow of communication from the aircraft to the operator placed at the ground station in a simulation environment would start from the detection of the threats which is done in the satellite terminals placed at the aircraft (two are needed in order to detect a possible hijacking of the SATCOM) which send the information to the satellite using the satellite link emulator. The satellite receives and process the signal to send it through other satellite link emulator to the Ground Base Station in order to display this information to an operator using a Human Machine interface where all the alarms, events and threats are displayed with more information, for example, location, severity, timestamp, flight ID, etc…

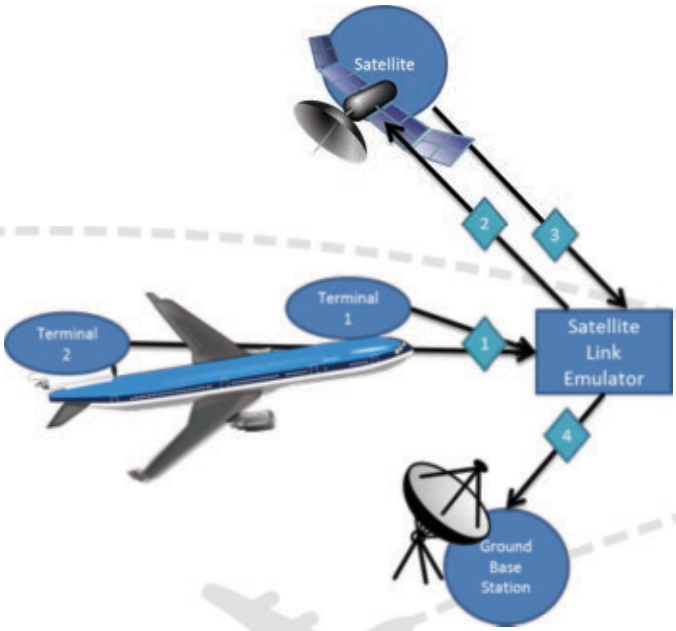


Figure 1. SATCOM Concept

Thales Alenia Space will use the knowledge acquired during the project to favor the definition and implementation of hybrid systems where SATCOM is part of a System of Systems. An example of this, is the implementation of smart antennas and hybrid networks

(terrestrial and satellite) used in SANSA or the research about new security and resilience solutions done in 5G-ENSURE, both of them part of H2020 European projects or the development of the PROGRESS (FP7 project), a TT&C link encryption solution to ensure TMTC information confidentiality, allowing secure data processing and high-speed direct control of payload elements from ground without going through the satellite's classical TT&C channel.

SATCOM ARCHITECTURE

To provide this functionality, the SATCOM security prototype consists of the following modules:

- AAA+: Will enable the SATCOM security manager to create/edit and assign the type of users and their clearance level to SATCOM resources, including their roles and responsibilities, to ensure among other things that any user of SATCOM resources sees only the ATM information that matches his/her clearance.

- Collector: Essential parameters to assess the status and quality of the ATM service via SATCOM, to evaluate the performance of the physical and logical resources, and to detect attacks at SATCOM assets.

- Networking: Will be responsible of direct or scheduled establishment/modification/release of ATM communications links via satellite as agreed and in coordination with IP/ATN/ACARS/ANSP.

- Supervision: This module is essential in the design and development of the SATCOM Security Prototype. It will detect, hierarchically list, suggest corrective measures and keep track of the faults that occur in any of the SATCOM Supporting Assets.

- Macros: Configuration and execution of automated operations on the SATCOM system as scheduled by the prototype's operator.

- Payload RF jamming detector: Detection of active interfaces and sniffing of the ATM data –traffic & signalling that is transmitted through the interfaces of SATCOM payloads to be able to identify and locate the source of RF Interference.

- HMI client: The client layer is the only who maintain contact with the prototype operator. In other words this layer contains the components that implement the human interface.

VALIDATION ACTIVITIES

The SATCOM Prototype was validated by Thales Alenia Space in a stand-alone environment at November 2016 involving different people of the company following several rounds of validations and verification processes using the Thales Alenia Space testbed in order to assure the performance and the quality of this prototype.

To validate the performance of the prototype, it was tested reproducing several inducted threats as DoS attack, Interception of communication, Management and Control Station (MCS) attack, Physical Damage, Radio Frequency (RF) interference and Satellite Control Centre (SCC) attack. The SATCOM validation campaign was performed within the Thales Alenia Space facilities in Madrid (Spain) through different attack scenarios.

The flow of the validation is illustrated in the following

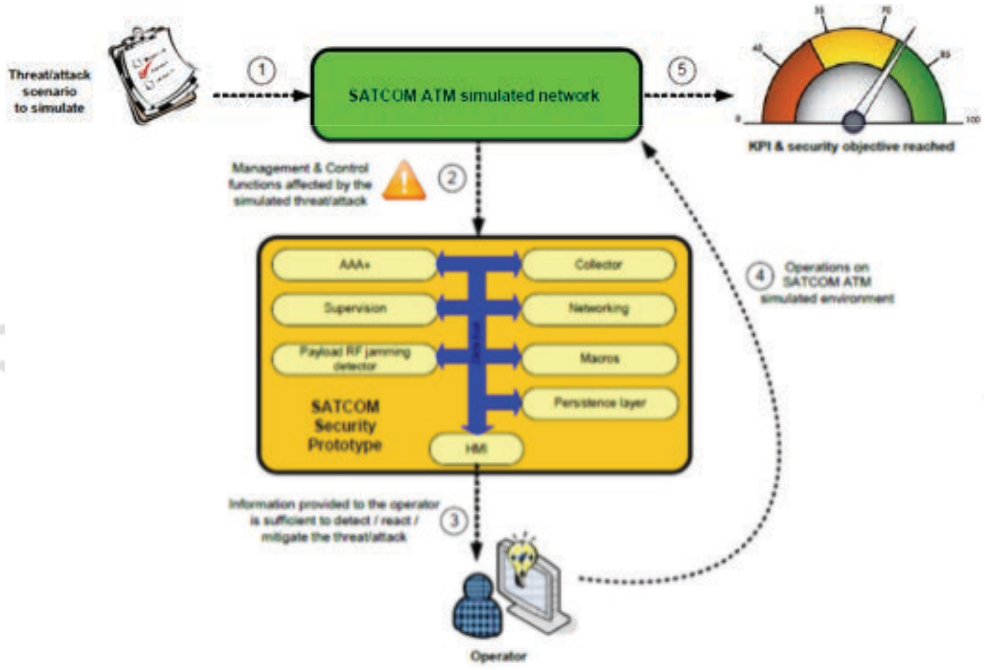


Figure 2. SATCOM validation

Figure (Figure 3), where can be seen the inputs and the outputs validation environment building blocks. The inputs were simulated at Thales Alenia Space facilities and the transition to the SMP emulator was developed using a VPN between Madrid and Italy for integration with the respective validation environment building block.

CONCLUSION

The GAMMA proposed solutions will contribute to the SATCom security advancement in the coming years. Currently security aspects in the standards are barely defined (as an example, for the DVB-RCS2 satellite interactive broadband European standard, definition of complete security solutions is still in starting phase) and are still far away from providing a strong security framework as planned to be delivered by the GAMMA project.

Knowledge on SATCOM security aspects gained through this project will boost Thales Alenia Space SATCOM secure solutions in the institutional, governmental and military market.

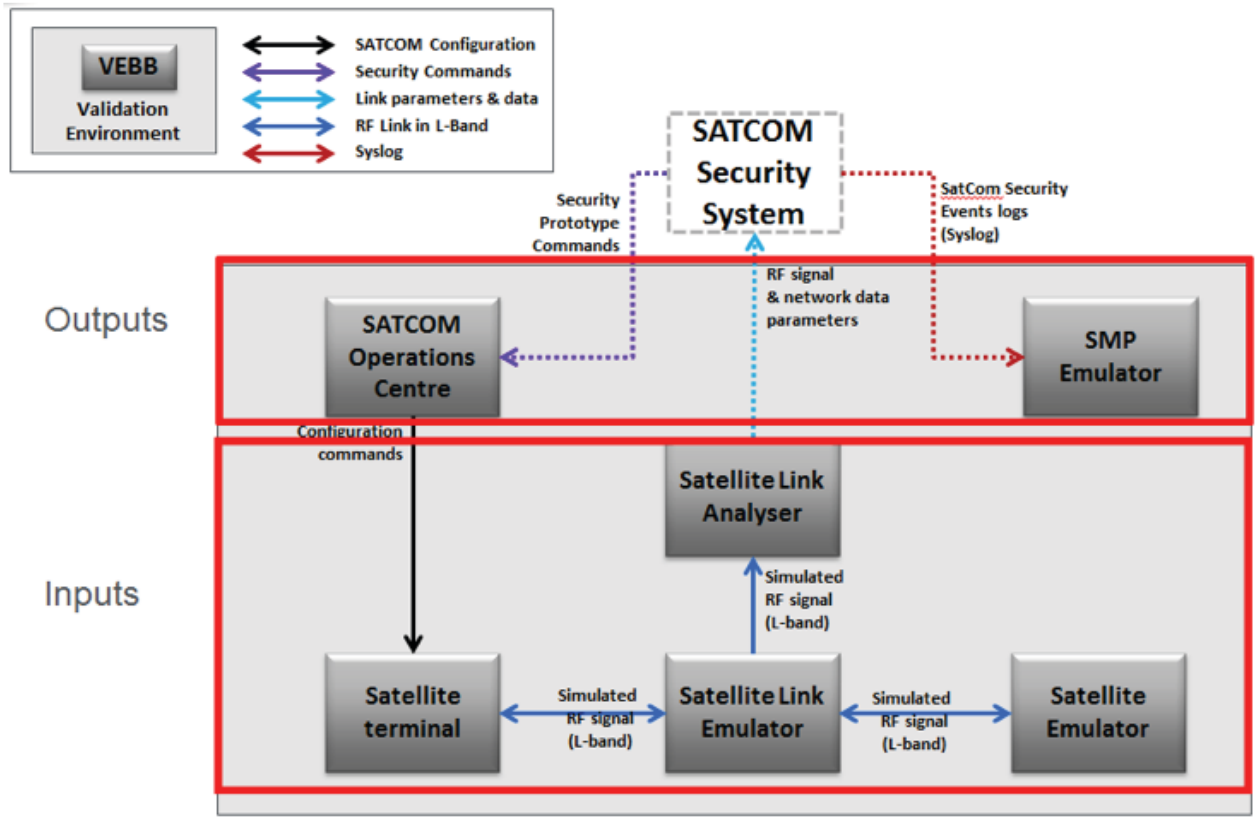


Figure 3. VeBB validation

The GNSS Monitoring System in GAMMA solution

***Bruno Montagne**, Thales Avionics*

I. INTRODUCTION

The GAMMA vision is to adopt a holistic approach to assess ATM security, in line with SESAR. GAMMA objectives are to:

- Develop a global ATM security management framework, representing a practical proposal for the day-to-day operation of ATM Security and the management of crises at the European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.

CNS based air traffic control increasingly relies on the use of GNSS not only for Navigation but also for Surveillance (for example, ADS-B uses GPS information). It is essential to detect GNSS interference or spoofing to secure ATM.

For Navigation, the evolution of the route structure and associated operations defined by the air navigation service providers is based on the extensive use of area navigation taking advantage of the capability of GNSS to provide worldwide accurate and monitored position.

The so called “GNSS solution” is used:

- on board aircraft for GNSS based area navigation and surveillance
- on ground infrastructures (as examples, GNSS are required for the GBAS ground stations, and it is also used for the WAM (Wide Area Multilateration) stations synchronizations)

GPS receivers are vulnerable to jamming and spoofing, the former being intentional or not. Such interferences have a high damage potential. The best known example of GPS jamming is the Newark incident, where air traffic was repeatedly disrupted due to a vehicle fitted with a personal privacy device regularly driving past the airport. Jamming and spoofing threats draw a growing interest from the scientific and industrial community.

This article is organized as follows: the first section introduces the GNSS risk assessment in ATM (GAMMA WP2). The second part details the architecture of the GMS (GNSS Monitoring System) developed for the GAMMA solution (WP4). The third part shows scenarios simulated to perform the prototype single validation and the results obtained (WP6).

II. GNSS RISK ASSESSMENT (GAMMA WP2)

In WP2 of GAMMA project, THALES avionics focuses on the specific aspect of GNSS use within the ATS. All services enabled through the use of GNSS have been listed and the effect of potential threats to GNSS has been described.

The Threat scenario assessment is evaluated in accordance with the SESAR ATM Security Risk Assessment Methodology defined in [SECRAM].

The GAMMA study focuses on interference threats targeted specifically at the airport and other threats indirectly disrupting ATC.

Today, jamming or interferences are commonly observed and spoofing is becoming a reality. The different threat use cases are analyzed in the following paragraph.

The Modeled threat scenarios affecting GNSS are identified as follows:

- GNSS jamming: jammer is close to the airport and GPS position becomes invalid,
- GNSS spoofing: fake GNSS signals are radiated to induce errors in the computed PVT

1. GNSS jamming

Two jamming scenarios in the vicinity of the airport are considered:

- A low power mobile jammer (e.g. a road vehicle fitted with a personal privacy device driving past the airport).
- A high power fixed jammer targeted at the airport.

The effects of each jamming threats are evaluated for the following situations:

- aircraft on approach,
- aircraft en-route,
- aircraft taxiing,
- ground vehicle taxiing,
- GBAS ground station,
- ADS-B (Automatic Dependent Surveillance-Broadcast) ground station,

• 10 WAM ground stations.

The first order effects are the same regardless of the platform: GPS position and time becomes invalid, but the consequences vary according to the use that is made of PVT information.

The following figure illustrates the area impacted by a single high power jammer aimed at an airport. The yellow square shows the area monitored around the airport. Red cells indicate GPS outage in that area.

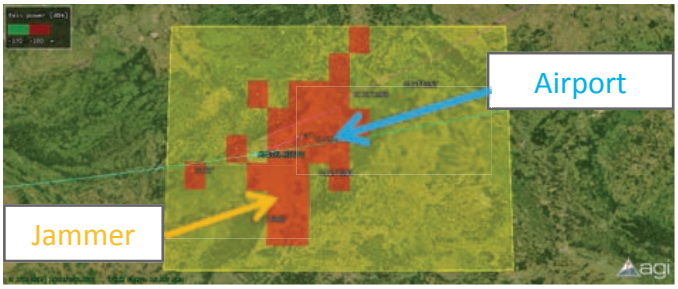


Figure 1: Power coverage with a stationary high power jammer

2. GNSS Spoofing

Three GNSS spoofing scenarios are considered: GPS signal spoofing, SBAS signal spoofing (SBAS navigation message), and GBAS signal (VDB datalink) spoofing. Consequences are the same for the three scenarios and depend on the spoofing detection.

III. SOLUTION ARCHITECTURE (GAMMA WP4)

The goal of the GNSS Monitoring System (GMS) is to detect, locate the origin and report GNSS spoofing and interference events. GNSS alerts are forwarded to the Security Management Platform (SMP) to support an overall security threat evaluation.

The architecture of the GMS is illustrated in Figure 2. It is composed of:

• GNSS sensors, which are located around the airport. Their role is to collect the GNSS signal and reception conditions and to forward the data to a GMS server. For the GAMMA project, GNSS sensors are simulated with a GNSS environment simulator (see Figure 3). Based on STK (System Tool Kit) and Matlab model. The GNSS environment simulator provides inputs to the GMS.

• The GMS secured server elaborates and stores information data which are provided to SMP (as GNSS alerts). The SMP then forwards the alerts to the relevant authorities such as ATC.

Figure 2 presents an overview of the GMS prototype with input/output interfaces:

• Output to the SMP (GNSS status and alerts) according to WP4 interface requirements.

• Input form GNSS environment simulator (signal propagation and GNSS sensors model) according to WP2 scenarios.

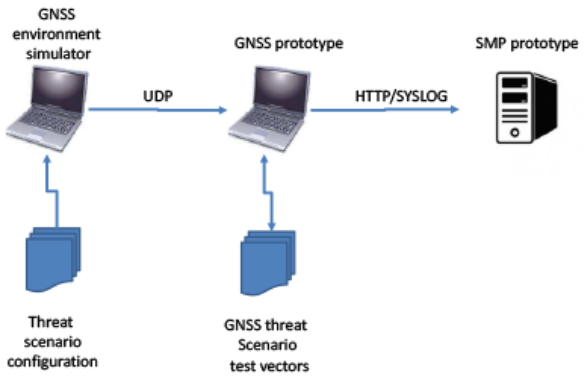


Figure 2 : GMS prototype overview

Figure 3: GNSS environment simulator

GMS determines if there is jamming or spoofing and then generates alarms accordingly.

An alert is sent to the SMP when jamming or spoofing is detected. Then, ATC is informed by GAMMA solution in order to take appropriate measures (e.g. cancel GNSS procedures) and information shall be send to national and European authorities.

IV. PROTOTYPE (GAMMA WP6)

Input of the GMS is limited to GNSS measurements which have been simulated with the GNSS environment simulator. The GMS is able to save input data so scenarios are replayed during the integrated validation exercise.

The GMS issues GNSS alerts to the SMP, which are decomposed into 3 messages:

• One message containing GPS sensor status information (GPS sensor position, jamming and spoofing indicator on each GPS sensor)

• One message containing GNSS alert information (date, jamming and spoofing indicator)

- One message containing jammer/spoofer information (jammer/spoofer estimated position and estimated power)

Alerts provided by the GMS are displayed on a graphical user interface (see Figure 4). Alerts messages are composed of the event start time and duration, interference classification (jamming or spoofing), and estimated jammer location.

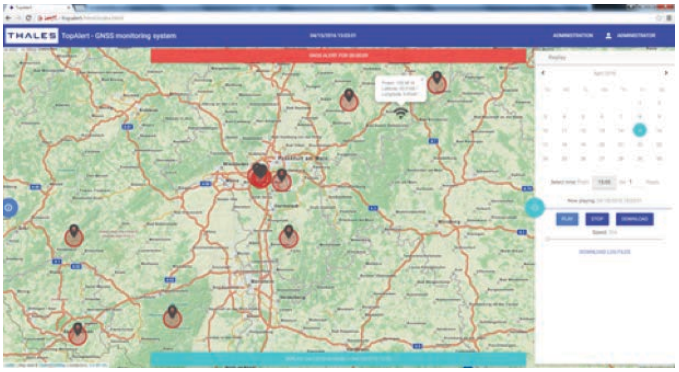


Figure 4: GMS HMI

V. CONCLUSION

GNSS Monitoring System developed on the GAMMA project allows detecting jamming and spoofing on a defined area and sending appropriate alerts to the SMP.

The TRL of the GMS server has grown to TRL 4 thanks to the GAMMA project.

VI. REFERENCES

[SECRAM] SESAR ATM SecRAM Implementation, Guidance Material, SESAR, 16.02.03 – D03, rev 00.02.06

Information Exchange Gateway (IEG)

Airbus CyberSecurity

Keywords: ATM, SWIM, SOAP, WSP, WSC, SQL Injection, XLM Bomb

I. INTRODUCTION

The GAMMA vision is to adopt a holistic approach to assess Air Traffic Management (ATM) security in line with SESAR [1]. GAMMA objectives are to:

- Develop a Global ATM Security Management framework, representing a concrete proposal for the day-to-day operation of ATM Security and the management of crises at European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.
- Design and implement prototype components of the GAMMA solution so as to demonstrate the functionalities and operations proposed for the future European ATM.
- Set up a realistic validation environment, representative of the target ATM solution, through which to perform validation exercises aimed at validating the feasibility and assessing the adequateness of the procedures, technologies, and human resources issues proposed.

II. CONTEXT

Next generation ATM system and more particularly System-Wide Information Management (SWIM) will be based on Services Oriented Architecture (SOA) principles driven by analysis of business processes.

The interface that allows ATM stakeholders to exploit, share and use the information in their own systems according to their own business, separates the information provision from the information consumption and is fully SOA compliant using web services technology.

Web services (WS) are versatile by design as they can be accessed by humans via web based client interface. They can also be accessed by other applications and other web services. Considered as one of the best ways to implement SOA, web services provide several technological and business benefits including application and data integration, versatility and cost savings. The combination of open standards protocols such as HTTP and XML-based protocols including SOAP and WSDL, allow exchanging data over intranets or internet in a very flexible way.

While providing new advanced business possibilities, web services introduce in the same way new significant security threats. The traditional security approach aimed at deploying IP packet filtering firewall solution which is not considered strong enough for the protection of web services. Indeed, web services need more sophisticated application layer firewalls being able to inspect packets deep into details and also to examine with more accuracy their payload.

III. IEG PROTOTYPE

The Information Exchange Gateway (IEG) is the prototype developed within GAMMA project (WP6) by Airbus CyberSecurity capable of detecting new kinds of offensive contents and intercepts them by deciphering, analyzing and confronting the messages with the access and filtering policy, and alerting the Security Management Platform (SMP).

The IEG serves to protect web services from XML-based threats like the injection of incoherent or spurious weather information or different kind of attacks against the SWIM system.

IV. HIGH-LEVEL ARCHITECTURE

In [2] [3] the design and specifications of the IEG and

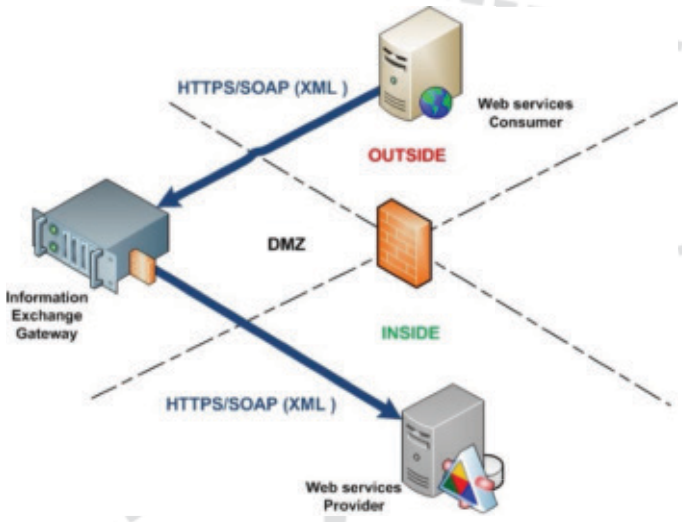


Figure 1 : High-Level Architecture

its environment is described. The IEG is placed in a Demilitarized Zone (DMZ), in face of the Web Services Provider (WSP) (see Figure 1). It scans ingoing-outgoing XML traffic in order to protect all assets for a perimeter given. Therefore, all requests coming from the Web Services Consumer (WSC) addressing the Web Services Provider (WSP) will be inspected by the IEG before they actually reach the WSP. In case the request content is not considered as malicious, it will reach the target. Otherwise, the IEG will drop the request.

V. MAIN FUNCTIONALITIES

The main functionalities of the IEG are:

- **Detection of malicious content**: It performs deep packet inspection (DPI) on SOAP messages to examine precisely the payload and the header. This kind of inspection allows the IEG to search for non-compliance protocol, malware, intrusions or other kind of malicious contents. It includes also rule-based detection methods and whitelist mechanisms combined with strict content validation policies.
- **Access control and encryption/ decryption capabilities**: The IEG supports authentication methods. It is compliant with WS-Security standards (authentication, signatures and encryption). It supports TLS (Transport Layer Security) for encrypting communications and mutual authentication (X.509 certificates).
- **Log alerting**: IEG registers every malicious SOAP transactions and evaluates and forwards the alerts to the SMP. The channel for transmitting alerts to the SMP is highly secured.

Since the IEG is at the heart of Web Services and the ATM, it must not be compromised. Thus, the functionalities have been built in a hardened system that uses file integrity check as well as offers a high level of robustness.

VI. IEG PROTOTYPE EXCHANGES

The IEG has to deal with different type of communications either coming from the internal network considered as trusted zone or from the external network considered as untrusted zone.

The connections the IEG has to deal with from the environment are depicted in Figure 2 and are listed as follows:

- **External interfaces**
  - Encrypted legitimate SOAP traffic
  - Potential attacks
  - Encrypted Syslog traffic
  - SSH traffic from CA (Certificate Authority)
  - Decrypted legitimate SOAP traffic
- **Internal interfaces**

Figure 2 : IEG and its interactions

VII. VALIDATION OF THE IEG AND THE ENVIRONMENT

A. Threat scenarios identification

Several threats scenarios have been identified as part of [4] [5] in which threats have been evaluated in accordance with the SESAR ATM Security Risk Assessment Methodology defined in SecRAM [6].

The following list of threat scenarios targeting SWIM has been identified and modeled in [7]:

- Injection of well-formed but incoherent weather information
- Injection of well-formed coherent but spurious weather information
- SWIM non integrity (spoiled DNS cache)
- SWIM SQL injection
- SWIM XML Bomb

Modeling threat scenarios has allowed identifying the actors involved in each threat scenario and their interactions and has ensured that the architecture solution actually covers the considered threats.

B. Validation Exercise

The validation of the IEG has followed the verification methods defined within GAMMA project [8][9][10][11] [12][13]. All functionalities have been validated taking the prototype as standalone as well as considering the integration with a whole validation environment that allows testing each of the functionality against a simulated environment close to the reality.

The validation plan specified the selected threat scenarios that have been used for testing the IEG in the validation environment.

The validation environment (Figure 3) is composed of the following essential assets:

- SWIM Network environment
- User web application interface to display weather forecasting to the user (Figure 4)
- Attacker platform providing a catalogue of real cyber-attacks
- Service registry including the UDDI directory
- Target ATM Stakeholder network

• Web Service Provider placed in the ATM Stakeholder network

The IEG validation exercise was designed to involve one test person and one cyber security engineer for the duration of one day.

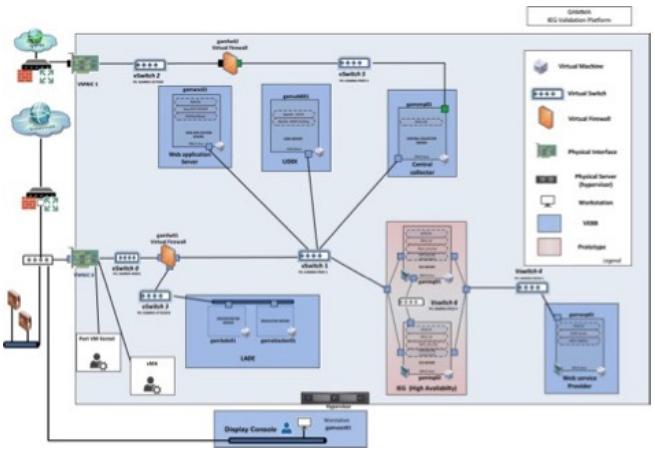


Figure 3 : Validation Environment

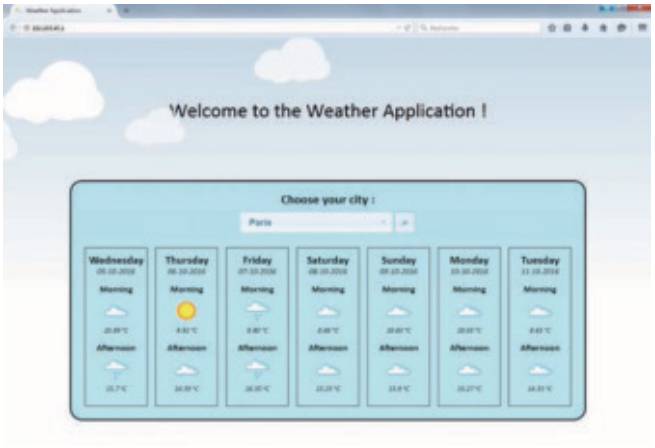


Figure 4 : Web Application Interface

Both persons did not need to have a comprehensive knowledge in air traffic control. The test person just had to be familiar with IT solutions and sensitized with cybersecurity aspects. The exercise has been conducted utilizing the platform designed for the validation of the IEG in which the selected attacks were launched against the WSP. The validations successfully met all the acceptance criteria and triggered all the KPIs identified for the evaluation of the IEG performance.

The IEG prototype has also been involved in an integrated validation exercise in which the prototype has been successfully tested together with other prototypes in a geo-distributed validation platform (Figure 5) [14]. In this fully integrated exercise a coordinated attack of international relevance took place. In here, a group of hackers were supposed to intrude the European SWIM (e.g. by using malware beforehand). The goal was to change Atmospheric Pressure at Nautical Height (QNH) values of local weather reports at selected major airports in two different European countries. The attack would cause safety problems due to incorrect altimeter settings of approaching aircraft. The IEG prototype reported the attack to National GAMMA Security Management Platform (NGSMP).

VIII. CONCLUSIONS

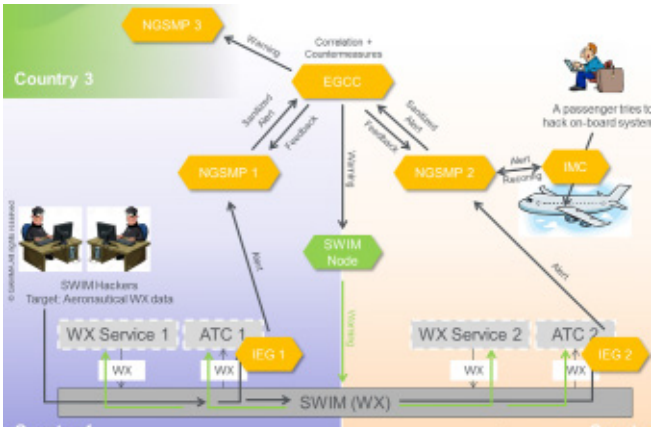


Figure 5 : IEG involved in the full validation exercise [14]

Next generation ATM system and SWIM tend to build its services relying on SOA. While providing new advanced business possibilities, web services-oriented architecture introduce in the same way new significant security threats such as SQL Injection (WSP database drop, WSP database modification, remote command execution…), XML Bomb (XML Generic Entity Expansion, XML Recursive Entity Expansion) or Local File Inclusion (XXE File inclusion), that can highly impact the operation of the ATM.

The IEG prototype validation has demonstrated the ability of the IEG to prevent WSP from being attacked.

IX. REFERENCES

[1] SESAR_Project https://ec.europa.eu/transport/modes/air/sesar_en

[2] GAMMA D6.2 Prototypes Requirements

[3] GAMMA D6.3 – Prototype Design & Development 1st Release

[4] GAMMA D2.1 – Threat Analysis and Evaluation Report

[5] GAMMA D2.3 – Risk Treatment Report

[6] Applying the SecRAM Methodology in a Cloud-based ATM Environment. International Conference on Availability, Reliability and Security, 2013.

[7] GAMMA D4.2 – ATM Solution Architecture Model

[8] GAMMA D7.1 – Validation Environment Requirements

[9] GAMMA D7.2 – Validation Environment Design & Development 1st Release

[10] GAMMA D7.4 – Validation Environment Integration Verification

[11] GAMMA D5.1 – Validation Exercise Plan

[12] GAMMA D8.2 – Validation Platform

[13] GAMMA D9.2 – Validation Report Full III

[14] GAMMA D9.1 – Release 1 Validation Report

Section 4. Validating ATM Security Solutions

Within this section a number of papers and articles are collected which discuss the validation approach of GAMMA. The application of security risk assessment methodologies and the validation of security prototypes and concepts are new to the domain of ATM. Therefore the insights and results of the GAMMA project regarding validation with focus on ATM security can be seen as a blueprint for future validations regarding security in ATM. The underlying methodology for the validation is the European Operational Concept Validation Methodology (E-OCVM), which was adapted and enhanced to meet the needs of a holistic security validation approach.

The first article gives an overview of the validation planning and explains the different challenges a validation in the ATM security domain poses. The reader is informed about the main tasks when setting up a validation plan and which mandatory cornerstones need to be respected when setting up security related validations in ATM.

In the second article seven different prototypes which have been developed in the course of GAMMA are described at a fairly high level. The reader is also introduced to the different approaches to set up the validations where also the roles of the participants and the different tasks are explained.

The next article is taken from a paper where one of the dedicated prototypes, the Secure ATC Communications (SACom), is introduced and the validation of this prototype is elaborated in detail. This section also presents some of the results of the security prototype validation conducted in the year 2016.

The following three articles explore the work done in GAMMA on the first security validations in ATM regarding single prototype validations as well as geo-distributed validation of different ATM security prototypes. This includes also the discussion of embedding the prototypes in their dedicated validation environment and complementing the validation platform.

One of the key contributions provided by the articles included in this section of the GAMMA publication is the definition of a kind of a blueprint proposed for setting up single security prototype validations as well as combinations of several security prototypes establishing sub-parts of a holistic security concept for ATM security.

***Tim Stelkens-Kobsch**, DLR*

Roadmap for the security validation

DLR

The GAMMA project is proposing a new operational concept to address security issues in the new global ATM scenario defined in SESAR. The Operational Concept includes roles and procedures for the day-to-day operation of ATM Security and the management of crisis at European level. This network-centric management framework needs support of technological solutions that facilitate the exchange of security information between stakeholders. Prototypes of those technologies are currently being developed in the project.

Therefore, the main objective of GAMMA is to complement the work done in the SESAR initiative, effectively addressing some security issues in the new global ATM scenarios.

The GAMMA vision is to adopt a holistic approach for assessing ATM security while maintaining alignment with SESAR. Indeed, when transferring this to the technical layer of project work some challenges arise. Focusing on the validation activities, the global objective defined for GAMMA, considering ATM as a system of systems environment and as a whole, cannot be entirely validated. Thus limitations to the validation of the holistic approach cannot be avoided.

The limitations for the validation mainly stem from the prototypes to be developed. Therefore the validation exercises will logically only represent a sub-set of the ATM system. Nevertheless, considering all validation exercises as a whole a more complete picture of the ATM environment can be evaluated on a higher level. This approach allows different validation goals depending on the target of the validation exercises.

As the European Operational Concept Validation Methodology (E-OCVM) states, validation can be a generic term with many meanings. Within the scope of GAMMA, the proposed definition of the E-OCVM for validation (which the European Commission agreed upon) will be applied:

“Validation is an iterative process by which the fitness for purpose of a new system or operational concept being developed is established. The E-OCVM focuses on providing evidence that the concept is ‘fit for purpose’ and answers the question, ‘Are we building the right system?’. In contrast to this, verification investigates the question ‘Are we building the system right?’”.

Using these definitions, verification would analyse if the system is built and running without error according to its specifications. The goal of a validation campaign is instead to analyse if the system is in line with the stakeholders’ expectations.

In the recent months since the issue of the first GAMMA newsletter the validation objectives of the project and a strategy for validations have been developed and formulated. The validation scenarios have been identified and the exercise plans defined. As stated above, the forthcoming GAMMA validation activities will collectively follow the procedure advocated in the European standard E-OCVM. However, the procedure is slightly adapted in some use cases in order to consider the experiences made by the partners within other projects. Thus, the GAMMA validation strategy is a combination of this well-accepted European standard and best practice.

Looking at one of the key elements of the project, namely the validation exercises, great progress has been achieved during the time span from the last issue of the newsletter.

Following reception of results from preceding activities (Risk Assessment, Risk Treatment, ATM Security Solution Architecture) the elaboration of all relevant input started in order to define the validation exercises as detailed as possible. The validation is strictly based on an ATM-security-incidents-centered approach which means that the validation scenarios are specified for the threats identified in the preceding work of the project.

E-OCVM means that the first step was to identify the validation needs. This very basic work was then followed by the identification of the needed validation activities, the validation strategy and the validation goals. The work was enriched by discussing and formulating the definition of the validation exercise plans and completed by elaborating a global cooperation of a European security system with non-EU security systems.

Every participant contributing to the prototype development has formulated the validation goals and the dedicated research questions as well for the particular prototype as for combinations of different prototypes.

The development of the dedicated validation scenarios was also done during the time since the last issue of the GAMMA newsletter. Validation scenarios were developed for the purpose of the validation activities and to gather evidence relevant to the validation objectives.

Validation scenarios are designed to focus on aspects of system behaviour which are of interest for the validation exercise. As each validation exercise has a different focus on specific aspects of the GAMMA solution, also specific validation scenarios are needed for each exercise. It is also likely that an exercise requires multiple validation scenarios (e.g. baseline validation scenario and solution validation scenario).

Herein a validation scenario describes the static properties of a run during validation activities. It includes the systems to be used and their configuration. The scenario also includes the (simulated) location (e.g. the characteristics of the simulated airport). In other words, the validation scenario includes all static characteristics of a validation run (see figure 1).

On the other hand, the dynamic characteristics of a validation run when carried out as a simulation are included in the simulation scenario. A simulation scenario in GAMMA consists of a traffic scenario describing e.g. aircraft movement, data exchanges, and other ATC events, and of a set of threats and their time of occurrence. The simulation scenario can be considered as a script for a validation run.

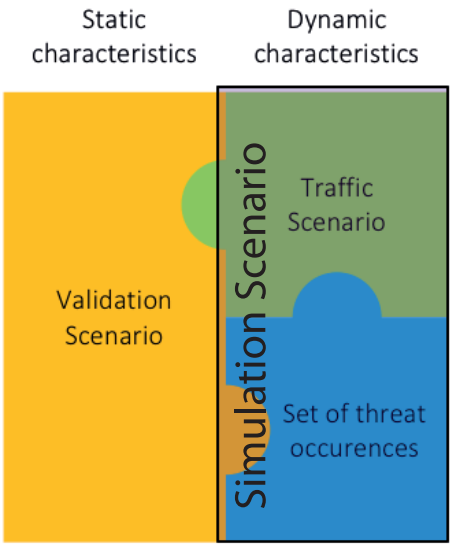


Figure 1: Illustration of the combination of a Validation Scenario, a Traffic Scenario and a set of threat occurrences as the setting for a run during a validation exercise

Traffic scenarios and sets of threat occurrences can be combined. Each possible combination results in a different simulation scenario. Also validation scenarios can be combined with different simulation scenarios, whereas a simulation scenario can be used with different validation scenarios.

The GAMMA ATM security solution establishes three different levels for managing security aspects: local (local security systems/centers), national (National GAMMA Security Management Platform, NGSMP) and European level (European GAMMA Coordination Centre, EGCC). The collaboration and information exchange between these different levels have to meet the national sovereignty requirements. The sovereignty requirements in turn mainly state that decisions related to national security only can be taken at national or local level. Thus, no decision can be enforced from the European level, but recommendations about actions or measures to be taken can be proposed.

In order to achieve the main GAMMA objectives (see figure 2) there will be a set of general (global) GAMMA validation goals (VALG) applied to all type of validation exercises. Linked to the latter ones more specific goals are specified (called strategy-related validation goals), which are applicable to each type of validation exercises. These goals depend on the validation approach chosen. There will be three types of strategy-related validation goals:

- Strategy-related VALG focused on the validation of individual prototypes,

- Strategy-related VALG focused on a partial integration of prototypes
→ event detector prototypes + national level of Security Management Platform (SMP) and

- Strategy-related VALG focused on a full integration of GAMMA solution
→ event detector prototype + National level of SMP + European level of SMP.

Figure 2: Validation Goals traceability path

Finally each individual validation exercise will define specific exercise objectives, which should be linked to at least one of the Strategy-related validation goals. Thus since the Strategy-related validation goals are in

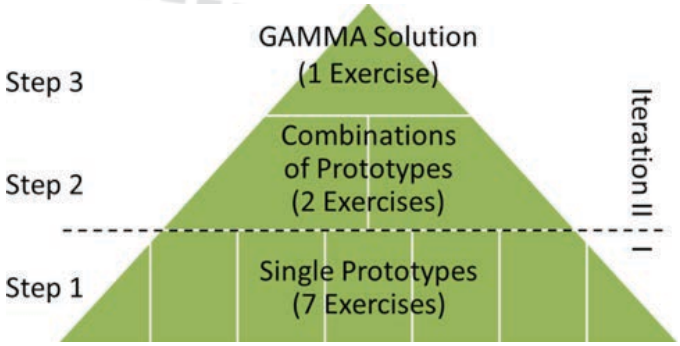


Figure 3: GAMMA validation strategy

turn linked to the GAMMA global validation goals, the traceability will be ensured allowing to assess the level of achievement of the GAMMA main objective.

Within the duration of the project three steps of validation activities shall be conducted (see Figure 3):

- Validation of all seven prototypes in single validations (7 Exercises)
- Validations of different combinations of prototypes on national level (2 Exercises)
- Validations up to the European level for the proof of the GAMMA concept (1 Exercise)

The mentioned combination of prototypes on national level is also called “partially integrated validation” (step 2 in figure 3), whereas the interconnection of prototypes up to European level is called “fully integrated validation” (step 3 in figure 3).

With the partial and fully integrated exercises the effect of implementing the proposed security concept on scenarios with coordinated and non-coordinated attacks will be investigated. This includes as well terrorist attacks on board of aircraft, attacks on ground based systems using different threats. Furthermore the effect on civil-military coordination in case of attacks on ATM systems will be investigated.

The validation work will be done in two iteration steps, where the first iteration (April 2016 – October 2016) comprises the single prototype validation exercises whereas the combined validation exercises will be conducted in the second iteration phase (March 2017 – July 2017).

GAMMA Prototypes and Validations

DLR

The GAMMA project was started with the ambitious goals

- to deliver and to validate a concept for a holistic and comprehensive ATM security management system and
- to develop and validate seven different ATM security prototypes on their own and interconnected with the others.

GAMMA is now drawing to a close and it is time to culminate the work in the final validations. These validation exercises are two fold, starting with a first series of validations focused on the prototypes in standalone mode followed by several partially and fully integrated exercises. This article gives an introduction to the seven prototypes designed and developed within GAMMA and describes the first series of validations.

The different prototypes designed and developed during the project duration are introduced hereafter.

Information Exchange Gateway (IEG)

The IEG enhances the traditional approach with a very strong mechanism of protection against most sophisticated attacks. IEG is capable of detecting new kinds of offensive contents and intercepting them by deciphering, analysing and confronting the messages with access control and filtering policies. Thus, it will serve to protect web services from XML-based threats. The IEG will be placed in a Demilitarized Zone (DMZ), facing the web service provider. It scans ingoing-outgoing XML traffic. All requests coming from the consumer addressing the provider will be inspected by the IEG before they reach the provider. In case the requested content is not considered as malicious, it will reach the target. Otherwise, the IEG will drop the request.

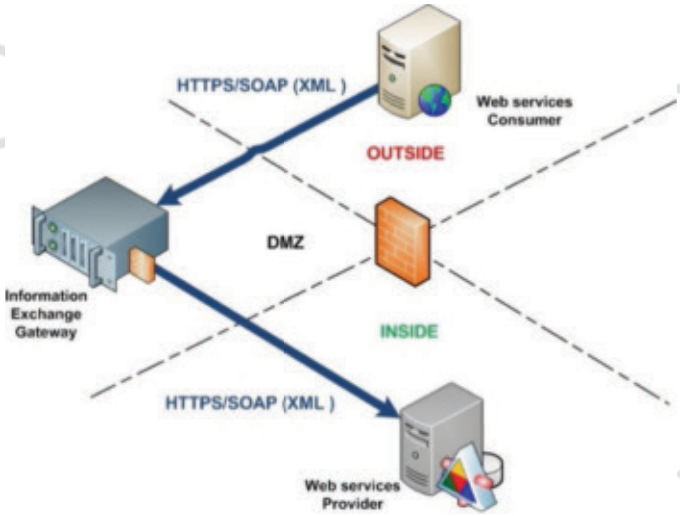


Figure 1: Information Exchange Gateway Positioning

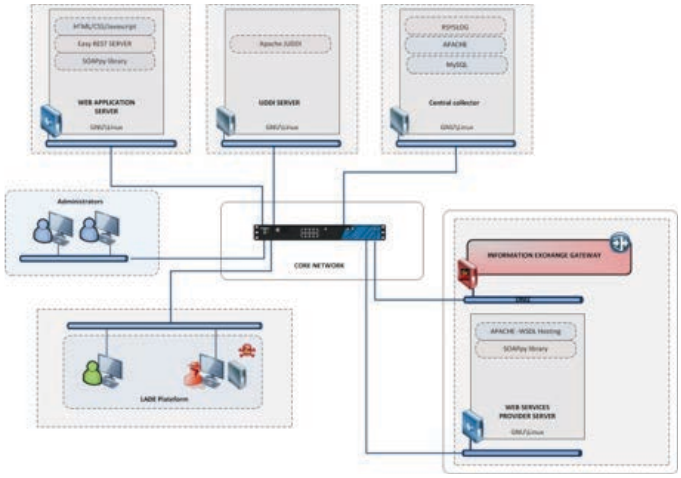


Figure 2: IEG validation platform

SATCOM Security (SATCOM)

The goal of the SATCOM security prototype is to detect and to offer countermeasures as fast as possible when a threat is targeting assets under concern. This holds true from the technical and/or operational point of view. The SATCOM security prototype is a client-server software solution designed to secure the management and control the communication in satellite networks. The impact of the threats targeting SATCOM assets is reduced by the coordinated functions of a set of modules integrated in the software of the prototype.

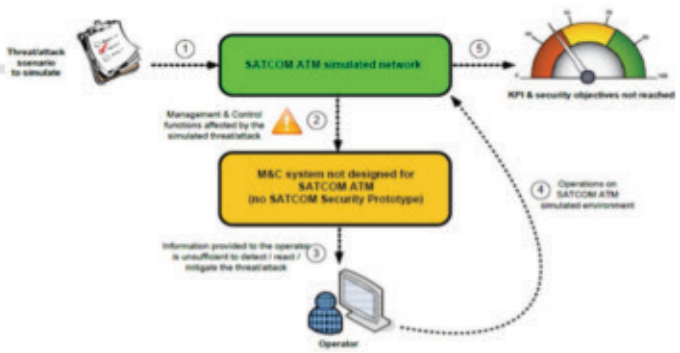


Figure 3: Without SATCOM security prototype

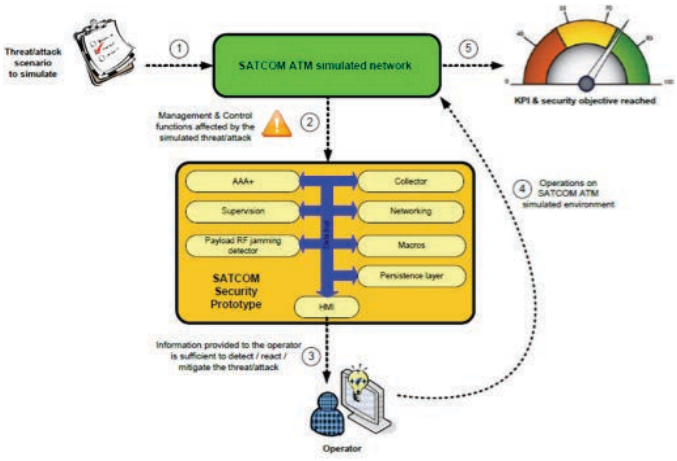


Figure 4: With SATCOM security prototype

Information Security System (ISS)

The ISS is composed of multiple systems integrated in the operational environment for Air-Ground Voice over IP (VoIP) ATC communications and data communication carried by the AeroMACS system. The ISS provides protected data communication on the airport side and for the Air-Ground (CPDLC and ADS-C) as well as Ground-Ground communications (PENS). The ISS also includes capabilities for communication and service authentication which enhances the required level of confidentiality, integrity and availability by mitigation of the threats. The ISS assists in identifying and monitoring suspicious activities and activates required countermeasures to minimize or avoid side effects on the communication and the air traffic network service.

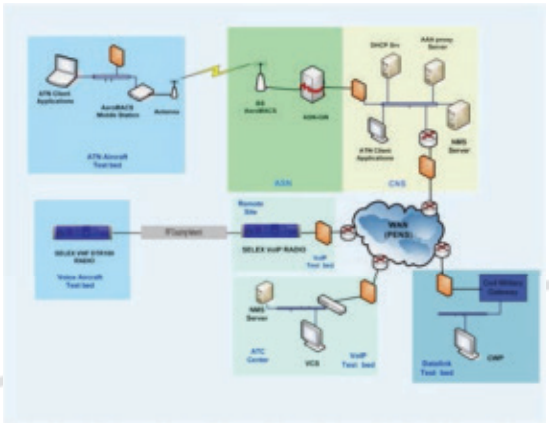


Figure 5: Information Security System

Figure 6: Aircraft in Florence Airport with a scheduled flight Plan to Rome

Integrated Modular Communication (IMC)

The IMC disseminates security alerts and may receive instructions for switching to different configuration depending on the security situation. These may be instructions to reduce functionality in response to an attack.

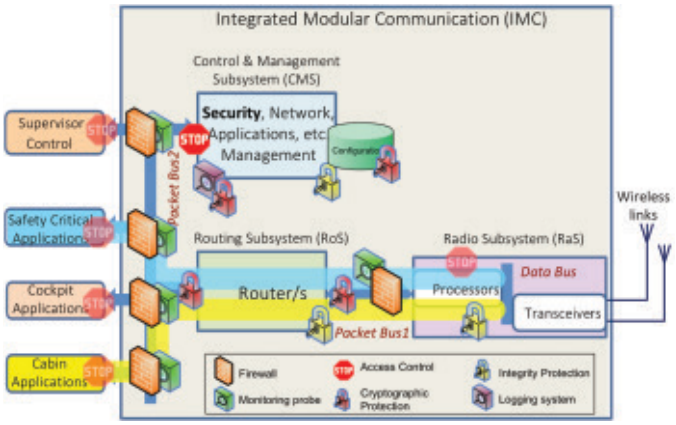


Figure 7: The IMC architecture with security controls

Secure ATC Communication (SACom)

The SACom Prototype in consists of three detector modules which perform speaker verification, stress detection and conformance monitoring. The different indicators are correlated and disseminated. The speaker verification module screens the voice communication and confirms authorization of speakers. The stress detection module also screens the voice communication and identifies abnormal voice patterns (e.g. induced by stress), which can be an indicator for unlawful actions. The conformance monitoring module uses electronically available clearances and surveillance data as input and checks if the aircraft flight trajectories correspond to given ATC instructions. Finally the correlation indicator module correlates all indications and forwards an overall threat indicator to the dedicated receiver.

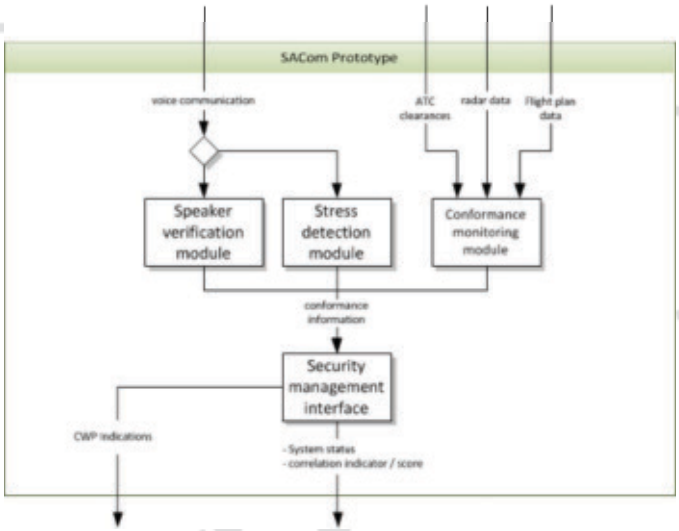


Figure 8: SACom Prototype architecture

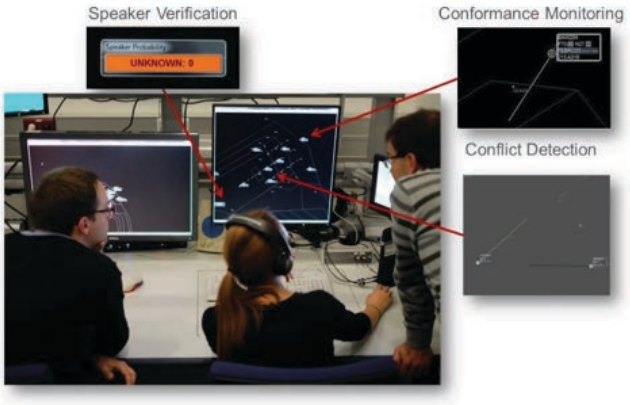


Figure 9: SACom Prototype

Secure GNSS Communication

The Secure GNSS prototype is able to detect GNSS jamming and spoofing. The system is composed of several sensors deployed on an airport and linked with a server easy to reach for ATC operators. Secure GNSS prototype provides an alert in case of interference detection with the GNSS signal to support an overall security threat evaluation. After receiving the alert about a threat from the system, ATC shall inform aircraft in approach to cancel GNSS procedures and information shall be send to national and European authorities.

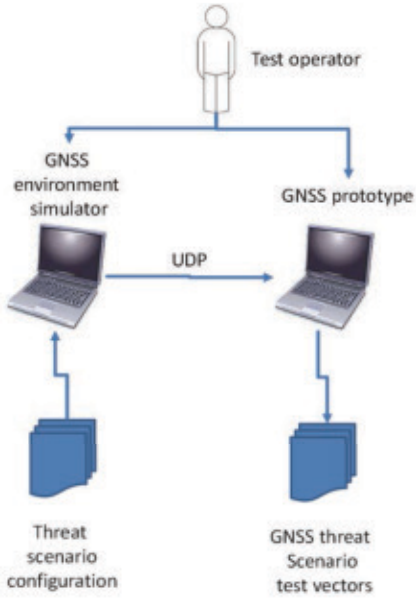


Figure 10: GNSS prototype overview

Security Management Platform (SMP)

The scope of the SMP is to provide Security Operators operating in the different ATM environments with a common overview on the status of ATM systems (situation awareness). The SMP collects information from event detectors connected to the different ATM systems, monitors and reports security events and incidents, and disseminates security information through a multi-level infrastructure that foresees instances of SMP at national level and a central SMP at European level.

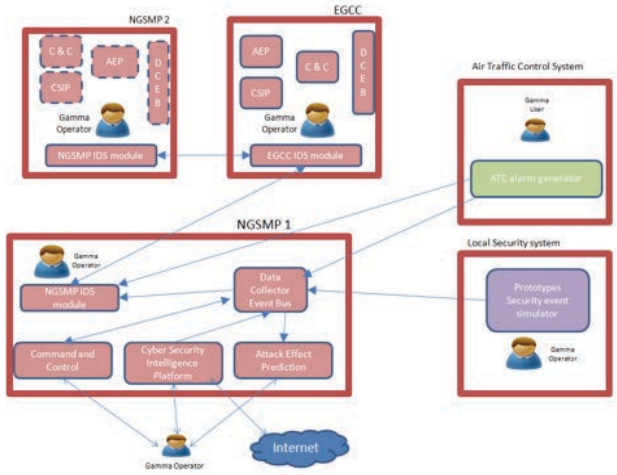


Figure 11: SMP validation exercise lay-out

VALIDATION OF THE PROTOTYPES

Information Exchange Gateway (IEG)

The validation exercise was designed to involve one test person and one cybersecurity engineer for the duration of one day. The test person took the position of the end-user and did not need to have a huge experience in air traffic control. The test person had to be familiar with IT solution and sensitized with Cybersecurity aspects. The cybersecurity engineer involved in the exercise did not need to have experience in air traffic control. The exercise has been conducted utilising the platform designed for the validation of the IEG. The validations successfully met all the acceptance criteria and triggered all the KPIs identified for the evaluation of the IEG performance. The IEG single prototype validation has demonstrated the ability of the IEG to cope with the threats that were identified in the Validation Plan.

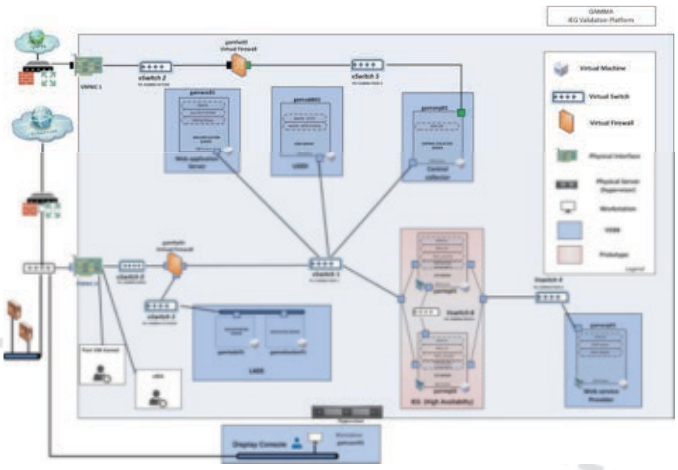


Figure 12: IEG validation platform

SATCOM Security (SATCOM)

The SATCOM validation exercises involved a test leader, a test person and observers. The duration of one exercise was not more than two days. The validation environment used can be divided into two parts; the first one to simulate the whole environment needed to create the most realistic environment for the SATCOM security

prototype and the second part (containing the SATCOM security prototype and the HMI client), which is needed to receive the alerts and perform the required actions by the SATCOM operator. The main result of the validation exercise show that without using the SATCOM, the number of false alarms produced were higher than the number of threat inductions (166,7%).

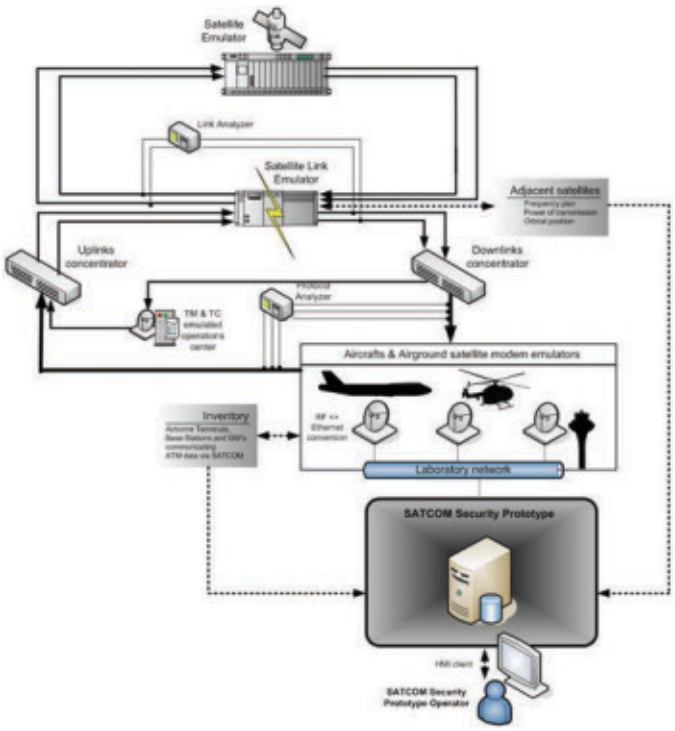


Figure 13: SATCOM validation platform

Information Security System (ISS)

The validation exercise of the ISS intends to involve the prototype in one or more operative scenarios with duration of about 60 minutes. Different scenarios have been executed and described in the validation result documentation. A test person, who takes the position of a Controller, Pilot and Security expert, was joining the validation exercises while an ATM domain expert and Network Manager Experts supervised the exercises. The security functionalities developed for the ISS prototype in the GAMMA project and tested through the stand-alone validation have achieved the required security objectives.

The ISS stand-alone validation exercise demonstrated these main results:

1. The test demonstrated that the vulnerability attacks have been identified and automatically blocked by the ISS IPS system using ISS Security Policies configuration.

2. The Network Security Manager was able to set and apply the new policies with the specific threshold value required to mitigate the security threats.

3. The vulnerability attacks performed on the ISS ground system didn't produce A/G communication loss.

Figure 14: ISS threats sessions detected and mitigated

Integrated Modular Communication (IMC)

The validation exercises of IMC have been performed on a windows PC. The IMC, IMC Traffic Generator (data traffic producer) and Security Management Platform emulator are all software modules and have been running on the same PC without the need for external communication links. The validation exercises have been conducted by an IMC tester. The tester initiated the running of various software tests by using the IMC Traffic Generator VEBB as well as performed some IMC administrator roles. During the validation exercise, three validation scenarios have been simulated following a time line. Namely an online attack to IMC through on-board systems, an online attack to IMC through off-board systems and an abuse of administrator privilege has been conducted. Customers require security that ensures the integrity of IMC by separating the different domains. The conducted tests validated the separation between the cabin and the safety domains, by showing that attempts to communicate between the domains are blocked.

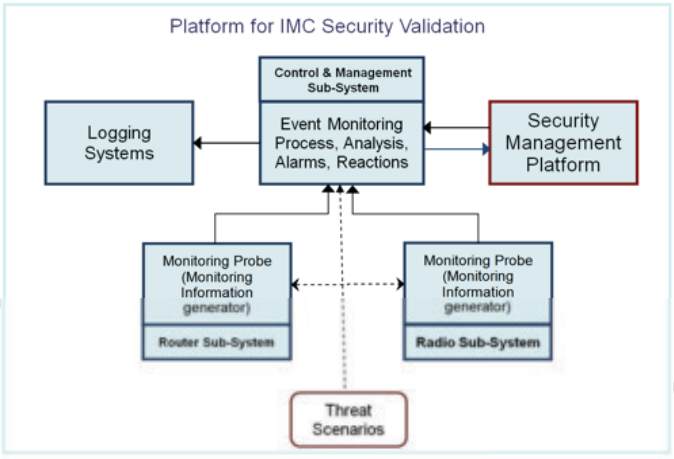


Figure 15: IMC Platform Configuration for Validation Purposes

Secure ATC Communication (SACom)

The validation exercise was designed to involve one test person for the duration of one day, while the supporting team to drive the simulations consisted of 5 persons. Due to the fact that security tests are typically just possible to be conducted if they happen with no advance warniong, the exercise was repeated multiple times, but with different test persons to avoid training effects. The test persons, who took the role of an ATCO, were recruited from the German Air Navigation Service Provider DFS.

The validation exercise consisted of a briefing, the enrolment of the speakers (to store the voice characteristics in a database), the validation of the enrolment, a training session to familiarise with the simulator, a validation phase with 20 short-time simulation scenarios containing specifically designed conflicts, a debriefing and a second validation phase with a simulated intrusion of an unauthorised attacker to the voice communication. The SACom validation campaign was performed within the ATMOS facility in Braunschweig. The activities showed, that match values of 90% or more are possible and where occasionally achieved for speaker verification by automatic voice analysis. Furthermore the conformance monitoring module also delivered very promising results. Unfortunately this is not true for the stress detection module which again proves the fact that detection of stress is still in its infancy. Nevertheless the invited ATCOs confirmed the added value the developed prototype would when experiencing security breaches like the ones which were considered.

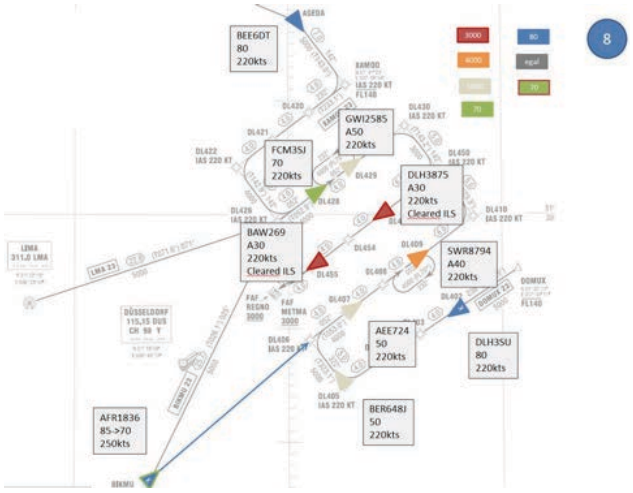


Figure 16: Briefing sketch for one short-time simulation

Secure GNSS Communication

The goal of the Secure GNSS Monitoring System (GMS) prototype is to detect GNSS interference or spoofing and to provide information to the SMP to support an overall security threat evaluation.ATC is then informed by the GAMMA system and subsequently informs aircraft in approach to cancel GNSS procedures. This information will then be sent to national and European authorities.

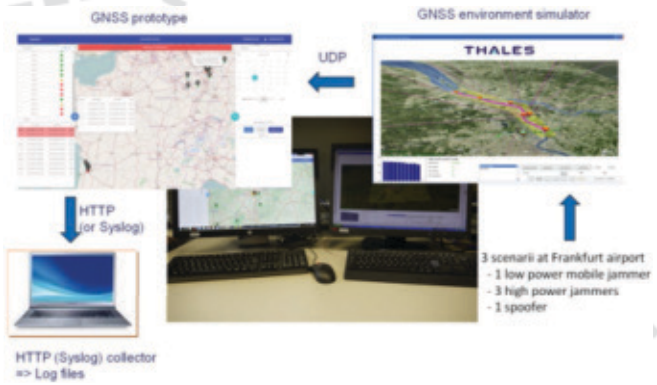


Figure 17: Single GMS prototype validation

Within the validation exercise one test person was involved to start and stop the simulation. This person did not need any kind of GNSS experience. Each validation exercise was planned for duration of one day and consisted of a briefing, the configuration of the GMS prototype and the conduction of the scenarios. The prototype showed its qualification to deliver the expected results.

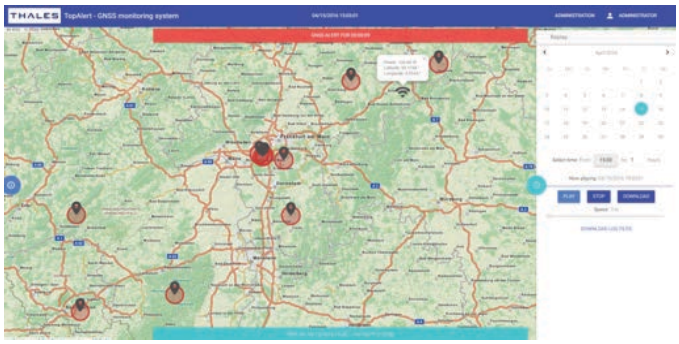


Figure 18: GMS prototype view

Security Management Platform (SMP)

Participants of the SMP validation exercise noticed the good visualising performance of the alarm on the Command & Control HMI. The offered function to obtain alarms due to a particular correlation of security events was seen favourable and the participants of the validation exercises noticed a good performance for dissemination of security information when alarm information needed to be transferred from a National GAMMA SMP (NGSMP) to European GAMMA Coordination Center (EGCC). Other functions such as a list of countermeasures (provided by the decision support functionality) were rated as a good support for the GAMMA operator.

The capabilities of the Attack Effect Prediction Module were considered to be very interesting. During the validations it appeared to be beneficial when some of the complex actions of the configuration phase are accompanied by a dedicated training. Furthermore the predictive capabilities of the Cyber Security Intelligence Platform were regarded to be of high interest because they provide the ATM system with information about possible attacks.

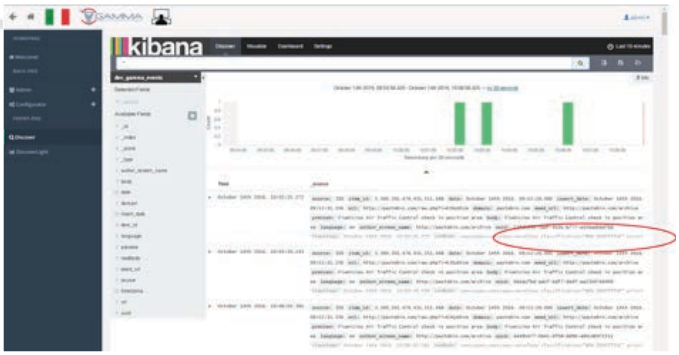


Figure 19: Security report displayed in NGSMP Command and Control interface

Validating an ATM Security Prototype - First Results

***Tim Stelkens-Kobsch; Michael Finke, Matthias Kleinert, Meilin Schaper**, Institute of Flight Guidance, German Aerospace Center (DLR) (Braunschweig, Germany)*

ABSTRACT

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

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

I. INTRODUCTION

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

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

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

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

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

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

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

II. BACKGROUND

A. GAMMA Project Overview

The GAMMA Project is one of the first European projects to address the growing importance of ATM security issues including new scenarios created by SESAR initiative. Besides identifying security threats and vulnerabilities,

possible mitigation actions shall be investigated and validated. The role of all affected ATM stakeholders as well as regulatory aspects, standardization and human factors shall be considered. To achieve this, a bandwidth of highly experienced project partners from research institutes (e.g. the DLR), universities (e.g. the Slovak academy of sciences (SAV)), industrial partners (e.g. Airbus DS, Finmeccanica, Thales) and subject matter experts (e.g. ENAV, ROMATSA, 42 Solutions) cooperate in GAMMA. The project started in September 2013 and will continue until August 2017.

B. Recent Research Activities

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

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

C. Security Risk 'Air-Ground Voice Communication'

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

D. System to be Validated

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

The system shall be developed as a threat detection system,

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

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

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

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

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

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

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

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

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

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

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

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

Primarily, SACom shall act as a threat detector to immediately and automatically send alerts to the SMP. With this automatism persons responsible for security

related decision making or management of security get the information immediately. Nowadays, this chain of reporting mostly relies on face-to-face or phone coordination, which takes some time until information are passed through and due to the large number of chain links there is a risk of loss of information.

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

III. VALIDATION METHODOLOGY

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

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

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

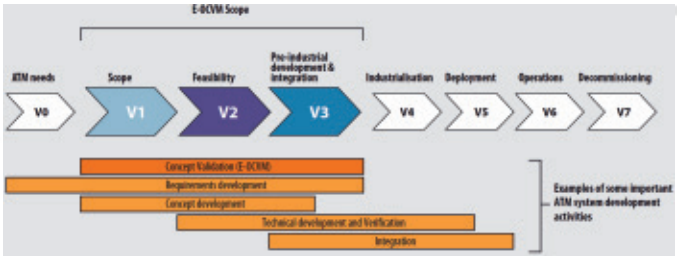


Figure 1: Lifecycle V-Phases [7]

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

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

A. Validation Goals

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

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

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

B. Validation Objectives

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

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

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

C. Key Performance Areas

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

D. Key Performance Indicators

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

E. Validation Requirements

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

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

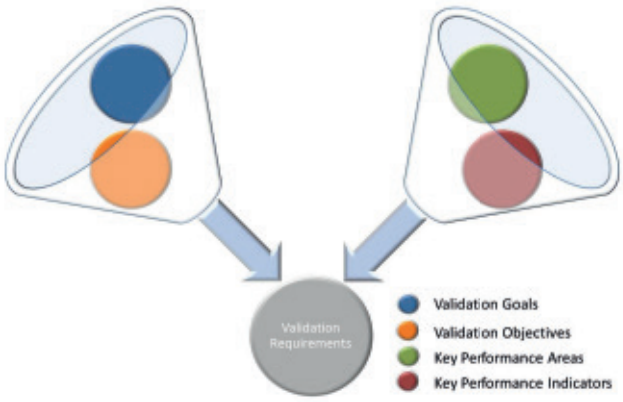


Figure 2: Composition of validation requirements

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

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

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

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

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

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

IV. VALIDATION APPROACH FOR SACOM

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

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

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

- The proposed prototype contributes in a beneficial way to the overall security management process.

- The information is available at the right place at the right time.

- Sensible information is only available for authorized roles.

- The information displayed to the user is considered usable, useful and beneficial.

• The detection of unauthorized participants in air-ground-communication is improved compared to a situation without the system.

• The system and related procedures can be implemented and used safely in the existing ATM.

• The performance of the SACom prototype is acceptable (regarding false alarms, correct detection, usefulness and trust).

• The SACom prototype leads to a better situational awareness of the ATCO as well as pilots regarding unauthorized intrusions into air-ground voice communication.

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

• Safety,

• Security,

• Capacity,

• Predictability.

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

• False alarm rate (Safety),

• Detection rate (Security),

• Number of detected dangerous / undesired aircraft behavior events in a defined time frame (Safety, Security, Capacity, Predictability),

• Recorded time until detection (Safety, Security, Capacity, Predictability),

• Number of unauthorized speakers detected in a defined time frame (Security).

B. Validation Requirements for SACom

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

• The validation environment shall provide a controller working position including all tools and assistance systems needed for the safe conduction of air traffic control according to present standards.

• A voice communication system simulating the air-ground voice communication shall be in place, which is equal in its handling to existing ATC radio communication equipment.

• Pseudo pilot stations shall be in place, allowing a realistic simulation of the pilot-controller interaction assuring realistic aircraft behavior and reactions.

• The validation environment shall allow real-time validation.

• Gathered data such as voice communication, prototype inputs and outputs as well as relevant events simulated during the exercise shall be recorded.

• Wherever a self-assessment or direct information from the test person is required, the validation environment shall allow him or her to state and record this information.

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

• The SACom prototype shall monitor the air-ground voice communication in real time and verify the authorization of all speakers by means of voice recognition.

• The SACom prototype shall monitor the air-ground voice communication in real time and detect voice patterns in the transmissions of all speakers which are typical for stressful situations.

• The SACom prototype shall provide means to monitor the compliance of all aircraft under responsibility of the ATCO to given clearances.

• The SACom prototype shall provide means to check if given ATC clearances do not induce safety-critical situations such as conflicts between two aircraft.

• The SACom prototype shall correlate all of the above mentioned indicators and provide status reports and alert messages, which are supposed to be sent to the SMP in live configuration.

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

• The interfaces between the SACom prototype and the validation environment building blocks shall use standard data formats (such as wav format for audio data or Asterix Cat 62 for radar data).

• Status reports of the SACom prototype shall be transmitted via a defined interface which is similar to the one used in live configuration with the same format / protocol.

C. Design of SACom Validation Trials

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

ATCO-centric exercises are performed as sets of Human-

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

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

D. Measurements and Data Gathering

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

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

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

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

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

V. FIRST RESULTS AND DISCUSSION

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

A. Speaker Verification

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

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

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

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

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

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

B. Stress Detection

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

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

C. Conformance monitoring

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

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

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

separation between aircraft. This means that, due to this pro-active countermeasure, aircraft deviations do not immediately cause a safety-critical situation when they act not conformant.

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

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

D. Correlation and reporting to the SMP

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

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

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

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

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

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

E. Conclusion – SACom prototype

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

- The robustness against a reduced audio quality must be improved significantly; especially when used for security reasons, where a very high reliability of the result is mandatory.
- Due to the unavoidable time span from the beginning of the transmission until the voice of the speaker is verified, the direct blocking of unauthorized transmissions or any other direct mitigation action is impossible. Following this, the system cannot be used to prevent the intrusion into the air-ground voice communication.
- Time delay from the beginning of the transmission until availability of final analysis must be shortened; if possible the result should already be available before the end of the transmission under analysis.
- Speaker verification results are only of minor usability if displayed at the controller working position; just alerts should be indicated.
- As the pilot is the person who is directly confronted with possible fake clearances from an unauthorized person, the speaker verification application may be more beneficial when available on the pilot side (i.e. aircraft cockpit).
- The speaker verification matching values are in principle meaningful enough to enable the pilot to distinguish between unauthorized and authorized transmissions. This indeed requires a continuously high reliability and accuracy of the analysis result; otherwise a significant safety risk could be introduced.

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

- The speaker verification as it is implemented during these trials requires an efficient enrollment management as there must be an enrollment for

every controller and every pilot who may be involved in controller-pilot voice communication.

• The system can easily be defeated by using recorded data from live ATC communication for the intrusion.

• The system will not detect an unlawful intrusion by a person who owns a valid enrollment and is listed as authorized speaker.

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

• The theory behind the stress detection is very complex and is still fundamental research. There is absolutely no experience for detecting stress patterns in the controller-pilot voice communication [15], and due to the large variety of stress-inducing factors (workload, safety issues, security issues, etc.), further research activities as well as the method of analysis must be more specific to the ATM context;

• A simulation environment is not fully suitable to validate stress detection. Real audio recordings or shadow-mode techniques should be used instead. In parallel, it needs to be investigated if and how persons executing unlawful actions show any kind of stress.

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

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

• The system needs an input methodology that ensures a fast and reliable input of every ATCO clearance.

• The use of conformance monitoring methods in combination with speech recognition of the ATC clearance proved as best suitable for this purpose and has the potential to be a very powerful instrument to quickly detect aircraft deviating from the instructed flight path (provided that the ATC clearance recognition rate is satisfying).

• Conformance monitoring alone is not an appropriate indicator for detecting an unauthorized speaker issuing fake clearances, as deviations can have different reasons (e.g. pilot action without clearance, wrong pilot action etc.); conformance monitoring does not distinguish between deviations caused by safety issues and those caused by security issues.

• Therefore there are rather safety benefits than security benefits as flight path deviations are typical for both, but safety reasons are much more likely.

• Highlighting the identified deviations in the corresponding radar can increase safety especially in high traffic load situations. Depending on the ATCOs awareness and workload it shortens the reaction time and helps to prevent after-effects.

• In order not to overload the radar display with deviation warnings, a filtering algorithm shall be in place which presents just the most urgent warnings.

• Deviation tolerances should be very strict for deviations from flight level, less strict for lateral deviations and may be quite generous for speed deviations, depending on the local needs.

F. Conclusion – Validation methodology

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

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

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

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

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

Regarding involved test persons, it is a big challenge to avoid expectations regarding the validations on their

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

VI. OUTLOOK AND FURTHER ACTIVITIES

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

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

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

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

The above will likely be materialized in subsequent prototypes. Lessons learnt are for example that research in stress detection needs first and foremost a fundamental definition of the state “stress”. Based on one tangible definition the measurement results can be assigned to a real or acted situation with more confidence.

The next prototype will also have an upgraded processing algorithm which allows receiving voice analysis while the speaker is still speaking. There will be no need for a distinct end of one phrase before the processing begins. These modifications will be done in parallel with developments dealing with increase of the size of the database holding the speech samples. Having said this it is also clear that special attention will always be given to use the SACom system in real time.

VII. REFERENCES

[1] www.gamma-project.eu

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

[3] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, C. Neeteson, „Towards a more secure ATC voice communications system“, 34th Digital Avionics Systems Conference (DASC), Prague, September 2015.

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

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

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

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

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

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

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

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

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

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

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

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

EMAIL ADDRESSES

{tim.stelkens-kobsch, michael.finke, matthias.kleinert, meilin.schaper}@dlr.de

The research leading to the results presented in this paper has received funding from the European Union FP7 under grant agreement no 312382. More information can be found under www.gamma-project.eu.

A Comprehensive Approach for Validation of Air Traffic Management Security Prototypes

A Case Study

***Tim H. Stelkens-Kobsch, M. Finke, N. Carstengerdes**, Institute of Flight Guidance, German Aerospace Center (DLR) (Braunschweig, Germany)*

ABSTRACT

Security in air traffic management is still a rather new challenge and receives increased interest during recent years. This implies that new security concepts and systems are developed. Usually all systems have to go through several validation cycles to reach a higher technical readiness level. As no well-established validation approach is available which considers the special aspects of security this forms an additional barrier when developing air traffic control security systems. This is true because suitable validation approaches have to be developed first. The latter includes the risk of forgetting something, when the development is not initiated in a structured way.

Within the air traffic security project GAMMA such an approach has been developed and applied to a set of seven prototypes. Based on the European Operational Concept Validation Methodology and a Security Risk Assessment Methodology, this approach identifies additional security controls, system requirements, validation objectives and key performance indicators. These are the driving elements for the design of the validation setup and procedure

The paper demonstrates the feasibility of this new approach using one specific example, the Secure Air Traffic Control Communications prototype.

The paper describes the approach and the resulting validation setup and procedures in detail. It briefly describes the obtained results for the developed prototype as one specific use case of the approach.

Keywords: Air Traffic Management; ATM security; validation; ATC voice communication

I. INTRODUCTION

Safety research and implementation of appropriate measures to ensure a safe flow of air traffic is well established throughout the air traffic management (ATM) for quite some time [1]. One might remember the long way necessary to establish the indispensable safety management system procedures in ATM (hazard identification, risk management, performance measuring, safety assurance …). From the security point of view, comparable security management standards do not yet exist. Thanks to endeavors of recent years, the gap between highly sophisticated safety related and security related ATM research, which is still in its infancy, could be narrowed in the future. There are several scientific and commercial projects and initiatives intended to increase security in ATM. [2] [3]. One of the research projects to pave the way to enhance ATM security is the Global ATM Security Management Project (GAMMA, http://www.gamma-project.eu/) funded under the 7th Framework Program of the European Commission. GAMMA takes input from as well the Single European Sky ATM Research Program (SESAR) as Next Generation Air Transportation System (NextGen) and is intended to bring theoretical ideas developed in recent years down to practical implementations.

Within the project seven different prototypes for enhancing ATM security were developed. One of them, called Security Management Platform (SMP), can be seen as the core element of the GAMMA security management concept [4] and was developed to collect, correlate and disseminate security information within nations, from nations to European level and vice versa. The other six prototypes reside more on the system level and are intended for directly securing defined areas of interest within ATM. The different prototypes are intended to be used e.g. in internet applications adopted by air traffic management, integrated modular radios, satellite communications, Data link communications, Aeronautical Mobile Airport Communication Systems (AeroMACS) and Air Traffic Control (ATC) voice communications.

The structure of this document reflects the strategy applied to successfully conduct validations of ATM security prototypes. This structure can be understood as a blueprint for future validations of single ATM security prototypes and of prototype systems. After this short introduction, section II initially describes the context from which the work origins. Section III then explains the approach of the Security Risk Assessment Methodology (SecRAM) [5], which was used for identifying assets, vulnerabilities and threats. Section IV describes the

purpose and design of a Secure ATC Communications (SACom) prototype as a technical example for an additional security control, whereas section V discusses the application of the SecRAM for this focus area in ATM. Section VI reports on the setup for the validation of the dedicated prototype. The validation is based on the well-known European Operational Concept Validation Methodology (E OCVM) [6]. Section VII discusses the results and finally section VIII gives some conclusions and a short outlook regarding the proposed methodology for validating ATM security systems.

II. CONTEXT AND SCOPE

A. Context

One feasible approach to describe the operational context when detailing the work conducted is to look from a management point of view. Management services in air transportation are categorized according to ICAO into Air Traffic Management (ATM), Communication, Navigation and Surveillance (CNS), Meteorological Services (MET), Aeronautical Information Services (AIS) and Search and Rescue (SAR). Fig. 1 depicts this context in an illustrative way (SAR is left out for simplification) [7].

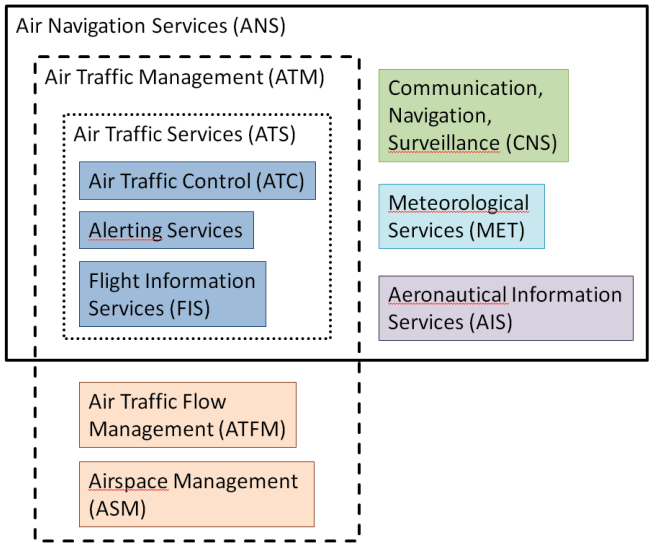


Figure 1: Components of ATM [7]

CNS/ATM is seen as the core service nucleus (or system) for the provision of air traffic management services (i.e. airspace management (ASM), air traffic flow management (ATFM), and air traffic services (ATS)) [8].

MET, AIS and SAR are considered as external to ATM (MET, AIS and SAR organizations are responsible for the security of their systems and functions themselves).

Interfaces to MET, AIS and SAR organizations and interoperability with associated systems fall within the scope of ATM Security.

In order to facilitate the understanding of the context the classification of different security topics will be carried out.

B. Scope

Fig. 2 shows a possible distinction between different focus areas of security. Fig. 2 has to be understood as a qualitative statement; the overlap areas are neither true to scale nor claiming completeness.

Aviation Security may be subdivided into ATM Security, Aircraft Security and Airport Security. The research presented herein will focus on the ATM Security

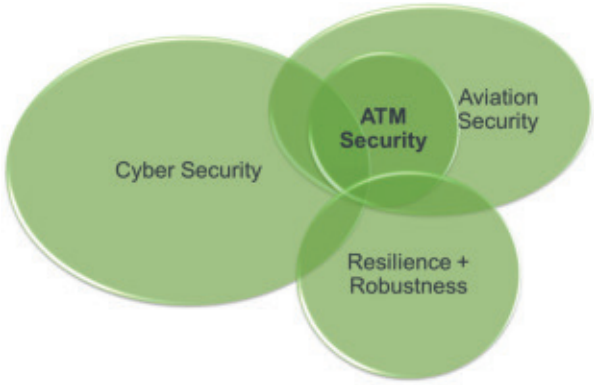


Figure 2: Relation of selected security areas

III. RISK ASSESSMENT AND TREATMENT METHODOLOGY

In order to describe the primary assets residing in the frame of ATM systems and being affected by attacks a thorough investigation has to be undertaken (see also [9]).

The procedural steps needed are guided by several methodologies. Following SecRAM (Fig. 3), two types of primary assets have to be taken into account: (1) services and (2) (primary) information.

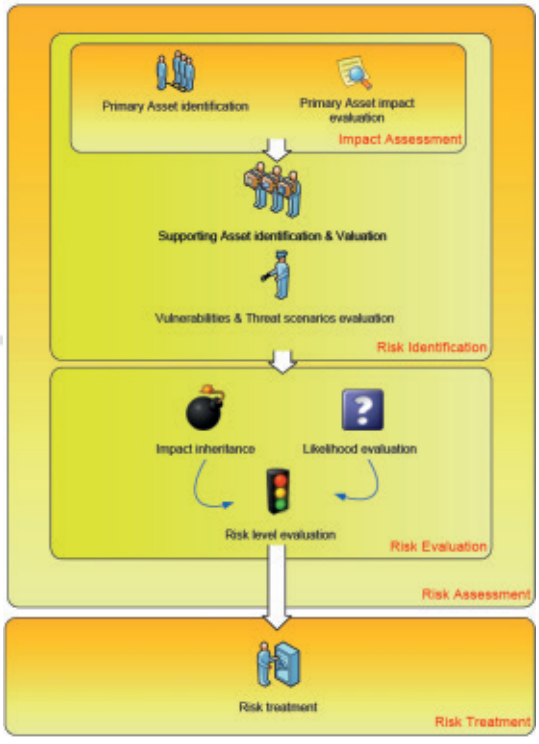


Figure 3: SecRAM process overview [5] [10]

(1) The services can be sub-divided in (a) services addressed by Operational Focus Areas (OFA), (b) system services, (c) operational concepts and operational activities and (d) necessary services to comply with contractual, legal or regulatory requirements.

(2) Information is considered as primary, when it is (i) vital for exercise of mission or business, (ii) personal regarding privacy, (iii) strategic or confidential and (iv) high-cost (regarding duration of acquisition or plain cost).

After the primary assets have been identified the possible impact on the level of Confidentiality, Integrity and Availability (CIA) has to be assessed (Table I). The impact has to be evaluated regarding both loss and degradation of the asset under investigation. In order to evaluate the consequences the security impact areas defined by SecRAM need to be used.

Hereafter the supporting assets need to be named. Supporting assets are tangible elements within the scope that support the existence of the primary assets. Typically these elements are e.g. entities involved in storing, processing and/or transmitting primary assets. Examples are servers, databases, laptops and workstations. In Air Traffic Control the voice communication can be seen as one of its supporting assets. The relation of supporting assets to primary assets may be described as 1 N (each supporting asset is linked with one or more primary assets).

TABLE I. IMPACT EVALUATION

Supporting asset	Impact evaluation									
	Threat	*Primary asset N*			*Primary asset N+1*			…	*Impact*	
		C	*I*	*A*	*C*	*I*	*A*	…	*Inherited*	*Reviewed*
SA #01	Threat #01	x		x		x		…	5	4
SA #01	Threat #02		x	x			x	…	3	2
…	…	…	…	…	…	…	…	…	…	…

TABLE II. LIKELIHOOD REGISTRATION

Supporting asset	Likelihood registration				
	Threat scenario	*Reviewed impact*	*Exposure level*	*Potentiality level*	*Rationale for parameters*
SA #01	Threat #01	5	4	3	This kind of scenario would trigger regional/national media attention. Expertise and knowledge required makes it somehow likely to occur.
SA #01	Threat #02	…	…	…	…
…	…	…	…	…	…

After identification of the supporting assets it is needed to reveal the vulnerabilities which could be exploited by adversaries. This step in the process inherits deep expert knowledge in order to identify the weak points in the ATM system. Now that vulnerabilities have been found the associated threats which endanger the system confidentiality, integrity and availability need to be conceived. Then the related risks that the prevailing vulnerabilities can be exploited have to be assessed. This is achieved by using the presented guidance material and obtaining expert knowledge. Thereafter the likelihood that the supporting assets are affected by a threat needs to be rated. This is done by using Table II and Table III.

TABLE III. LIKELIHOOD EVALUATION

Supporting asset	Likelihood evaluation		
	Threat	*Reviewed impact*	*Likelihood*
SA #01	Threat #01	5	3
	Threat #02	5	2
SA #02	…	…	…
…	…	…	…

With Table III the likelihood that a threat occurs is considered and rated. Table IV is then intended to estimate the risk level (low, medium, high) by taking into account the previous considerations. Presented here is a snippet of the table, which was established within the GAMMA project.

TABLE IV. RISK LEVEL EVALUATION

Supporting asset	Risk level evaluation			
	Threat	*Reviewed impact*	*Likelihood*	*Risk level*
SA #01	Threat #01	5	3	High
	Threat #02	5	2	High
SA #02	…	…	…	…
…	…	…	…	…

The resulting risk values are now composed in a matrix, which is called risk level evaluation (Fig. 4).

This risk matrix can be used to define needed measures for reducing the risk appetite and scaling down the likelihood that a threat is successful (risk treatment). Furthermore the impact of a successful threat can be decreased. The pending steps are now to postulate security objectives to secure the assets. The security objectives represent the measures chosen when working with the risk matrix. This means for each asset of concern one or several security objectives are identified. The security controls shall ensure that remaining residual risks still existing after the treatment meet the postulated security objectives for the assets. For the GAMMA project this is documented in [11].

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Figure 4: SecRAM risk matrix [5]

The risk treatment needs to be supported by well-known catalogues of generic descriptions of security controls. In aviation a preferred suggestion is to use e.g. the Minimum Set of Security Controls (MSSC) developed by SESAR [12]. After the risk minimization effect of these controls has been rated, there might be a residual risk. This residuum now is treated by additional security controls (ASC), which are systems, assets or procedures

not yet existing. At this point the need for postulating new security prototypes and/or procedures arises. Within the research project GAMMA for example this evaluation led to the development of seven different ATM security prototypes developed by different partners of the project. The detailed approach chosen for the application of the SecRAM methodology in GAMMA is shown in Fig. 5 and documented in [13]. The numbers represent the quantity of items identified.

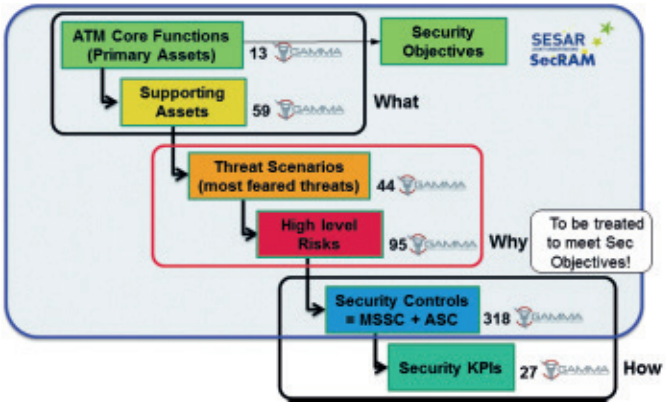


Figure 5: Security Risk Assessment and Treatment in GAMMA [14]

The prototypes mainly focus on separate subdivisions in ATM. Six of the prototypes reside on system level and one prototype is intended to collect, rate and disseminate the information received by the others. The latter is called SMP, (briefly described in section I). The six system level prototypes are (1) Information Exchange Gateway (IEG), (2) SATCOM Security, (3) Information Security System (ISS), (4) Secure GNSS Communication, (5) Integrated Modular Communications (IMC) and (6) Secure ATC Communications (SACom) [15].

In the remainder of this paper the application will be demonstrated by taking the SACom prototype as a specific example. The SecRAM application provides the basis for the intended development of a security prototype validation methodology.

In order to set the scene the reasons for the development of such a prototype will be explained.

IV. THE NEED FOR SECURE ATC COMMUNICATIONS

The rationale for developing a security prototype in the area of ATC voice communications is underpinned by the fact that radio communication used by ATC can easily be intruded and has therefore been subject to recurrent attacks [16] [17] [18]. Nevertheless the voice communication between pilots and air traffic controllers is still the basic and most important communication method within the aeronautical mobile service, as it is the most flexible and efficient medium especially in a busy traffic environment or when non-standard situations occur.

The communication via voice is therefore one of the supporting assets of ATC. Although the use of data link is steadily increasing, it can only partly replace air-ground voice communication and cannot be used in time-critical and/or non-standard situations with current datalink procedures. For example, CPDLC is not designed for aerodrome control, approach control or VFR flights and does not provide sufficient response times [19].

The international voice communication standards in aviation involve the use of omnidirectional analogue radio transceivers with double-sideband and amplitude modulated carrier waves. The VHF frequency band range is defined with 117.975-137.000 MHz [20].

The commonly known characteristics of analogue omnidirectional radio voice communication resulting from wave propagation physics can be summarized as following:

- Requires line-of-sight to a certain extent (e.g. a ground-based transmitter may be received by an airborne radio but not by another ground-based receiver; the same airborne transmitter is most likely received at both ground stations (Fig. 6)).
- Simultaneous transmissions on the same frequency cause interference making both transmissions (almost) unreadable (so called "block-out").
- The reception quality decreases with increasing distance to the transmitter (nearby stations may outgo stations of a larger distance).
- Due to the analogue nature, modern encryption technology cannot be used.

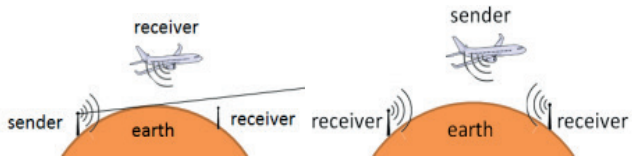


Figure 6: ATC Voice Communications [21]

As a conclusion, the still widely used analogue air-ground radio voice introduces a significant security risk:

- Physically, the current unsecured air-ground voice communication can be freely accessed.
- Appropriate radio communication equipment to access the air-ground voice communication is available for purchase with almost no restriction.
- Any unlawful interference, especially those that appear to be credible transmissions, may remain undetected for a certain time.
- Any interference directly influences the provision of Air Traffic Control Service and therefore also directly endangers the assurance of preventing collisions between two aircraft or between an aircraft and another object and of maintaining a safe, expeditious

and orderly flow of air traffic.

Possible security threats targeting the air-ground voice communication (see Table I – IV and [10]) are:

- Intentional frequency blocking/jamming,
- Fake transmissions to airplanes by unauthorized persons (in the following referred to as "False ATCO", i.e. False Air Traffic Controller) with the goal to severely disturb the safe and orderly flow of air traffic. Such fake transmissions are not necessarily received by Air Traffic Control due to the effects described above.

The SACom prototype addresses the second one of the above mentioned security threats. Recent examples for this kind of unlawful interference were reported in [16] and [18] and impacts were investigated in more detail in [16].

This prototype consists of several modules providing the following functions:

- Verification of all speakers in air-ground voice communication by analyzing voice characteristics ("speaker verification function").
- Determination of the current stress level by analyzing stress-typical voice characteristics in air-ground voice communication ("stress detection function").
- Trajectory-based and state-vector-based conformance monitoring to detect aircraft deviating from given ATC clearances ("conformance monitoring function").
- Trajectory-based and state-vector-based conflict detection ("conflict detection function").
- Correlation of the functions above as a basis for automatic reports to security management instances.

V. APPLYING SECRAM FOR SACOM

The above described methodology has been applied and the primary and supporting assets have been identified for the validation of Secure ATC Communications. The primary assets which need to be protected (or at least parts of) were found as:

- Communication service.
- Arrival management and landing procedure.
- Pre-departure sequencing, departure management and take-off procedure.
- Conflict management (separation/collision avoidance).

After the primary assets have been determined the following step was to identify the supporting assets. The result of the determination is shown below:

- Voice system.
- En route Area Control Center (ACC).
- Each approach control unit.
- Each aerodrome control tower.

Subsequently the threats able to exploit the vulnerabilities of the supporting assets needed to be imagined. This appears to be the most critical part in the risk assessment, which also requires a high level of expert knowledge about the functionality of the supporting assets.

For these threats a detailed investigation regarding impact evaluation, likelihood registration, likelihood evaluation and risk level evaluation has been conducted following SecRAM [5] and described in section III, which provides the described set of tables to fulfill this task.

In the first risk treatment step the security controls already in place need to be named by identifying them from a catalogue of pre-described controls. Such a catalogue is, for instance, inherited in the MSSC.

Taking the mitigation effects of those more general security controls into account there may be not enough success to reduce the risk level to an acceptable value. However, this can be further enhanced by proposing adapted general security controls (taken from the MSSC) or additional security controls which need to be invented from scratch. When implementing these controls it is assumed that the risk level is mitigated to acceptable values (i.e. low or medium). The needed ASC to achieve the mitigation are listed in Table V.

The list of additional security control drives the postulation of requirements for the validation setup. The prototype can now be developed and verified according to these constraints. Hereafter the validation exercises can be planned.

TABLE V. SECURITY CONTROL LIST SACOM

Supporting asset	Security control list		
	Threat	*Security control ID*	*Control description*
Voice system	False ATCO	ASC_TFA_01	Air-Ground voice system shall change to digital radio communication which provides means to encrypt messages
	Freq. blocking	ASC_TFB_01	
Voice system	False ATCO	ASC_TFA_02	Air-Ground voice system needs a restricted access to hardware
	Freq. blocking	ASC_TFB_02	
Voice system	False ATCO	ASC_TFA_03	Air-Ground voice system shall use message encryption
Voice system	False ATCO	ASC_TFA_04	Each ACC/TWR shall provide means to detect unusual trajectory of flight
Voice system	False ATCO	ASC_TFA_05	Air-Ground voice system shall be supported by means to detect voice pattern anomaly
Voice system	False ATCO	ASC_TFA_06	Each ACC/TWR shall operate and control speaker verification
Voice system	Freq. blocking	ASC_TFB_06	Air-Ground voice system shall have the possibility to increase transmitting power of transmitter

VI. VALIDATION SETUP

Within the GAMMA project the SESAR guidance material available for risk assessment and treatment has been applied straightforward. The consecutive step was then to apply also the E-OCVM to plan and execute tailored validations in a structured way. The combination of these methodologies delivers the inevitable blueprint for the validation of ATM security prototypes.

According to the GAMMA Validation Exercise Plan [22] (which was written using the guidance of E-OCVM) the functionalities of the SACom prototype are proven by validating the single prototype in standalone configuration. Following the E-OCVM, system requirements and, in the following, the validation objectives were derived.

In order to develop distinct security validation scenarios, the baseline was defined as the existing operational concepts and system functionalities with respect to security. Against this baseline, the GAMMA benefits were demonstrated and validated.

In order to validate any requirement, Key Performance Indicators (KPI) need to be defined which provide a measurement of efficiency to weigh e.g. the benefit of an additional security control and to assess if security objectives (e.g. performance of the prototype, acceptance, enhancing of situational awareness) are fulfilled. Several indicators and values were determined during the validation trials (see also [23]):

- Performance of the prototype's speaker verification function (Detection Rate/False Alarm Rate).
- Performance of the prototype's stress detection function (Detection Rate/False Alarm Rate).
- Performance of the prototype's conformance monitoring function (Detection Rate/False Alarm Rate) as well as the air traffic controllers performance practicing the monitoring function without any support (Detection Rate).
- Performance of the prototype's conflict detection function (Detection Rate/False Alarm Rate) as well as the air traffic controllers performance practicing the conflict detection function without any support (Detection Rate).
- User Acceptance.

The definitions of detection rate and false alarm rate in this context are depending on the application area of each prototype module and will be detailed in the results and discussions part

The chosen validation method for the SACom prototype was Human-in-the-loop (HITL) simulations. Within the study six air traffic controllers participated with more than ten years of controllers' experience, four of them were male. Five of the participants were mid-aged experienced German ATC center controllers, whereas one controller was a mid-aged person and experienced as well in Australian as Irish ATC centers. Each person under test acted as an ATCO and was confronted with many different events, caused by security and/or safety problems. As a prerequisite to conduct the validation exercises voice examples of all persons under test needed to be recorded (a so called speaker enrollment).

The validation exercise duration was 8 hours, spread over two days. The exercise started with a briefing, introducing the research topic and also explaining the goals of the general security concept. However, the participants were unaware about the False ATCO threat and the validation questions of the following exercise runs. Afterwards, the ATCOs had to be enrolled and authorized in a speaker database for the SACom prototype. Then the participants had about 20 minutes to familiarize with the simulation and their controller working position. During the remainder of day one, the participants acted as approach controllers in 20 short scenarios with duration of about five minutes each. In some of these scenarios different threats occurred and the ATCOs had to cope with them. In the background and unnoticed from the participants the SACom prototype was running and thus creating both baseline data together with performance data from the participants. On the second day the SACom prototype was explained to the participants without mentioning that in the following exercise scenarios a False ATCO attack will be performed. Hereafter a training scenario was performed where the participants could test all functionalities. Afterwards there was one simulation run of 45 minutes duration, where the SACom indications and warnings were visible to the participants and False ATCO attacks were performed. Afterwards a long debriefing was conducted which included several questionnaires.

As a summary, one complete exercise consists of the following steps:

1) Briefing of the participants
2) Speaker verification enrollment and enrollment test
3) Simulator training (no SACom indications visible)
4) 20 short simulation scenarios (no SACom indications visible)
5) SACom Briefing
6) SACom training simulation (SACom indications visible)
7) False ATCO attack simulation (SACom indications visible)
8) Debriefing and questionnaires

VII. RESULTS AND DISCUSSION

A. Performance of the Speaker Verification Function

The speaker verification function of the SACom prototype delivers a score value (ranging from 0 to 100) for each transmission of any speaker. Authorized speakers usually showed speaker verification scores of 40-70 while unauthorized speakers usually showed scores of less than 30.

Validation exercise step 2) was used to determine the optimum alert threshold for unauthorized speakers (transmissions with a measured speaker verification score values at and below the alert threshold are considered as unauthorized).

For evaluation the following definitions have been taken:

- The detection rate was defined as percentage of all unauthorized transmissions which were detected as unauthorized transmission.
- The false alarm rate was defined as percentage of all authorized transmissions which were wrongly classified as unauthorized transmission.

The results shown in the Table IV were obtained from approximately 100 utterances spoken per exercise run involving all speakers of the exercise (three authorized and one unauthorized speaker).

The values in Table VI have been gained under the following conditions:

- All speakers had no secondary tasks during this exercise step and had the opportunity to fully concentrate on giving the utterances.
- No time constraint was present.
- A limited number of utterances were considered.
- The used Voice over IP (VoIP) audio system provided a very high audio quality.

TABLE VI. SPEAKER VERIFICATION RESULTS

Exercise Run	Aircraft conformance – Detection Rate		
	Optimum Alert Threshold	*Detection Rate*	*False Alarm Rate*
1	15	100%	3.3%
2	14-30	100%	0%
3	27-35	100%	0%
4	21	96.0%	0%
5	31-40	100%	0%
6	33	91.7%	0%

Recapitulating the results presented above, a very high reliability is shown (very high detection rate of about 91.7% to 100% and very low false alarm rate of about 0% to 3.3%). Provided that the system is robust against the named factors, the potential to apply the speaker verification algorithms of the SACom to air-ground voice communication is clearly visible. This is true especially to directly detect unauthorized transmissions in the frame of the above mentioned threat scenario.

It has been observed that the time difference between the end of the transmission and the display of the result plays a critical role for the usability of this function because a human operator must always be able to correlate the audio transmissions with the indications. If the time difference between both events is too large a human operator will not be able to identify which utterance caused an alert.

During the exercises, a default alert threshold setting of 30 was used as a first estimation. After completing the run, the alert threshold were be adjusted to achieve the best results. This optimum alert threshold shows differences from exercise run to exercise run. Hence, an alternate solution needs to be found to (continuously) adapt depending on the actual constellation of speakers and used audio equipment.

Another constraint is the speaker enrollment. This voice example should have a length of 3-5 min of continuous speech and should be recorded with the audio equipment that is going to be used in the radio conversation. Factors like fatigue, stress or sickness as well as a reduced audio quality had significant influence on the performance of the speaker verification function in the exercises. For implementing this function in the existing air-ground voice communication a solution has to be found for managing the speaker enrollments for a very large number of authorized participants and either the audio quality of radio communication or the robustness of the used speaker verification function has to be improved.

B. Stress Detection Function

The stress detection function of the SACom prototype delivers a stress score for each transmission of any speaker. The stress score is determined by searching for stress-typical voice patterns according to a database of stressed speech. The value of the stress score should directly reflect the experienced level of stress. Validation exercise steps 3) and 7) were used to obtain stress scores within simulations were it is expected that the speakers are relaxed (to determine a false alarm rate) and within simulations were it is expected that the speakers are under stress in some predefined situations (to determine a detection rate).

The detection rate was defined as the percentage of all transmissions which are assumed to be under stress and which are correctly classified as stressed transmissions.

The false alarm rate was defined as the percentage of all transmissions which are assumed to be free of stress and which were wrongly classified as stressed transmissions.

At first it has to be mentioned that in the frame of the project it was not possible to check the success of the stress induction by using well-established means like psychophysiological measures or questionnaires, as the resulting effort and budget was not covered.. This fact has to be kept in mind when interpreting the results.

Usually the determined detection rates are below 30% with a large variation between the different exercises. The determined false alarm rates show the same trend (false alarm rates of up to 30% with large variation between the different exercises. The reliability of stress detection based on voice pattern analysis as implemented with the SACom prototype may directly depend on the voice characteristics themselves; the reliability may then differ from person to person.

According to the statements above, further research is necessary to raise the stress detection to a mature state. One of the most important steps would be the creation of a database of stressed and unstressed controller speech samples to extract typical voice stress patterns in ATC (controllers and pilots). Such a database is far away from being available.

C. Conformance Monitoring

The conformance monitoring function of the SACom prototype delivers an indication for each aircraft when the system detects a deviation from the given clearance. This function needs precise, correct, complete and actual information about given clearances, which can be gathered e.g. from highly sophisticated speech recognition tools. This would avoid incorrect, missing or late clearance inputs which jeopardize correct functioning.

Validation exercise step 4) was used to obtain the performance of the prototype and of the air traffic controller monitoring the traffic without any assistance. This was done by carefully reviewing simulation recordings and correlating the deviations detected by SACom with the traffic situation.

1) Detection Rates

The detection rate (for both SACom and ATCO performance) was defined as the percentage of existing aircraft deviations which were correctly detected by the prototype resp. the air traffic controller.

Table VII shows obtained results for the detection rates.

TABLE VII. CONFORMANCE MONITORING DETECTION RATE

Partici-pant	Aircraft conformance – Detection Rate		
	ATCO Detection Rate	*SACom Detection Rate*	*Difference SACom - ATCO*
1	92.0%	88.0%	-4%
2	76.7%	93.3%	+16.6%
3	91.7%	95.8%	+4.1%
4	80.0%	96.7%	+16.7%
5	84.6%	88.5%	+3.9%
6	85.0%	85.0%	0%

The distribution shows that the system performance is basically equal or higher than the performance of the air traffic controller. This shows the potential of conformance monitoring assistance tools in general both from the security and the safety point of view.

Simulated events which the controller frequently did not notice were:

- Level deviations (because - in contrast to lateral deviations which are directly visible on the radar screen - the controller has to read and process the altitude information displayed in the radar label).
- Deviations which do not directly conflict with the preplanning of the air traffic controller.
- Deviations of aircraft which do not yet need any guidance (in the used approach control simulation e.g. shortly after handover still far away from the airport).

One short simulation run contained a planned level deviation during the final leg of the ILS approach, induced by a simulated false advice from an unauthorized speaker to discontinue approach, climb on runway heading flight level 70. All six controllers did not detect the deviation in time, as a level deviation was unexpected after the aircraft reported to be established on the final approach. The situation ended in 2 near-miss situations and 4 mid-air collisions with another approaching aircraft (Airborne collision avoidance systems were not simulated). This underlines the severity of such a security threat.

2) False Alarm Rate

One feasible possibility to determine a false alarm rate is to calculate the number of false alarms divided by the number of all alarms. In doing so a false alarm is defined as an alert by the prototype's conformance monitoring system without any deviation of the considered aircraft from the spoken ATC clearance. This approach has been chosen for evaluation of the conformance monitoring to be the most appropriate.

The false alarms can be categorized by carefully reviewing simulation recordings and pseudo pilot command logs. Two types of false alarm rates can be defined:

- False Alarm Rate Type 1: Number of false alarms including false alarms caused by incorrect, missing or late clearance inputs divided by the number of all alarms,
- False Alarm Rate Type 2: Number of false alarms excluding false alarms caused by incorrect, missing or late clearance inputs divided by the number of all alarms.

Table VIII shows the results for the false alarm rates. It is obvious that the system is very vulnerable against wrong, missing or late clearance inputs, causing a high number of false alarms (e.g. participant 2 had a false alarm rate type 1 of 71%). After these errors have been eliminated, it can be seen that roughly 10% of all alarms are false alarms (mainly caused by simulation errors), which would be acceptable.

This underlines the need for a very reliable method to

precisely and quickly capture the spoken ATC clearance. In this validation exercise, speech recognition technology which is available at the German Aerospace Center (DLR) research facility in Braunschweig was used. This speech recognition technology showed very high recognition rates in former validation trials [24] [25]. According to the results presented here, this can be considered as the absolute minimum required performance for using speech recognition technology together with monitoring tools in general. This underpins the need to use the all modules of SACom in combination to achieve a system which can increase the security level in ATM.

TABLE VIII. CONFORMANCE MONITORING FALSE ALARM RATE

Partici-pant	Aircraft conformance – False Alarm Rate	
	False Alarm Rate Type 1	*False Alarm Rate Type 2*
1	63.8%	10.3%
2	71.0%	7.2%
3	34.2%	2.9%
4	56.7%	9.0%
5	58.9%	12.5%
6	52.8%	11.1%

3) Average Time until Detection

The average time until detection was determined for the SACom prototype as well as for the Air Traffic Controller without any technical support. For every single aircraft deviation, the time difference between the simulation timestamp at which the deviation was visible for the first time on the radar display and the simulation timestamp at which the system or the air traffic controller recognized the deviation was determined. Finally, the average was calculated over all single deviations for every exercise run, which is summarized in Table IX.

These results clearly show that an automatic monitoring system – provided that it is fed with complete, reliable and valid clearance information – is able to detect aircraft deviations much faster than an air traffic controller. In these experiments, the system was always between 20 and 30 seconds faster than the unsupported air traffic controller. There were several situations during the simulations where it would have made a significant difference in safety to detect the event 20 seconds earlier. This shows again the potential of conformance monitoring tools in general.

TABLE IX. CONFORMANCE MONITORING TIME UNTIL DETECTION

Partici -pant	Aircraft conformance – Time until Detection		
	ATCO Average Time until Detection	*SACom Average Time until Detection*	*Difference SACom - ATCO*
1	41.6 s	16.5 s	-25.1 s
2	39.4 s	11.8 s	-27.6 s
3	43.1 s	15.8 s	-27.3 s
4	38.7 s	14.5 s	-24.2 s
5	38.9 s	13.9 s	-25.0 s
6	34.7 s	14.1 s	-20.6 s

D. Conflict Detection Task

The conflict detection function of the SACom prototype delivers an indication for each aircraft constellation where the system detects a risk of a loss of separation. Besides the "classical" conflict detection according to the actual speed vectors, the SACom prototype also uses context information to predict aircraft trajectories. Similar to the conformance monitoring function this needs precise, correct and complete information about given clearances.

Validation exercise step 4) was used to obtain the performance of the prototype and of the air traffic controller searching for possible conflicts without any assistance. This was done by carefully reviewing simulation recordings and correlating the conflicts detected by SACom with the traffic situation.

A conflict was defined as a situation where the usual minimum IFR separation in approach sectors (3NM lateral separation and 1000ft vertical separation) is not ensured within the next 60 seconds.

The detection rate (for both SACom and ATCO performance) was defined as the percentage of existing conflicts which were correctly detected by the prototype resp. the air traffic controller.

The false alarm rate was defined as the number of SACom conflict alerts without any real conflict situation as defined above (taking the latest ATC clearances into account) divided by the number of all SACom conflict alerts.

During the simulation runs, the conflict detection function of the SACom prototype showed a similar performance for the detection rate as the air traffic controller. The average detection rate over all exercise runs for both was about 85%.

The false alarm rate for the SACom prototype showed values between 0% and 20%.

E. User Acceptance

The air traffic controllers taking part in these exercise runs gave their feedback and were asked to fill out both bespoke and well-established, standardized validation questionnaires. These questionnaires covered not just the rating of SACom but also about the simulation setup, realism, the GAMMA concept and also questions about ATM security in general.

Exemplary, Fig. 7 shows an extract of the results obtained for the user acceptance. The blue pillars show the mean ratings while the black brackets show the standard deviation of the answers.

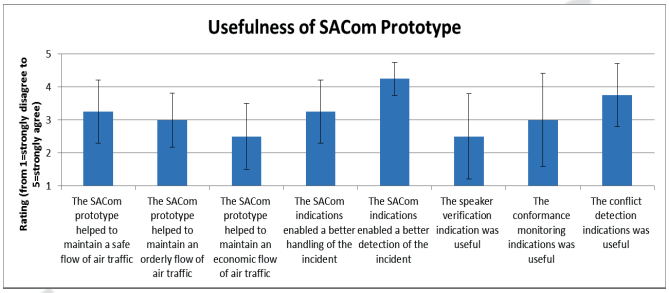


Figure 7: User ratings obtained from questionnaires

The obtained data show a general agreement to the approach taken with the SACom prototype. A closer inspection of the available answers reveals that there is a clear trend in the data concerning a distinguished view of the various modules of the SACom prototype. The Conflict Detection module always gets the best assessment, followed by the Conformance Monitoring module. The Speaker Verification Module was rated as the least useful feature, mainly due to the chosen method of presentation and not regarding the function as such (speaker verification results were presented in an additional window and showing every verification result and not only unrecognized speaker alarms). This feedback will be taken into account for the further development of the HMI of the prototype. It has to be noted that the neutral opinions of the participants regarding statements concerning the safe and orderly flow of traffic and the slightly negative remarks concerning an economic flow of traffic cannot be seen as a negative result. Rather this result was expected as the prototype was meant to enhance security without the intent to improve the safe and orderly flow of traffic. According to the participants the economic flow of traffic suffered a little bit, however, this comes as no surprise and was expected as a security trade-off. In summary, the participants agreed that the SACom prototype enabled a better detection of the False ATCO attack and is a preferable solution to secure ATC voice communication.

No questions were asked concerning the stress detection feature, because stress detection results were not displayed to the controllers during the exercise.

Summarizing the results of the extensive debriefing sessions, the participants had a positive view of the SACom prototype and its modules, seeing benefits of the prototype itself and the GAMMA concept in general for improving ATM security. The concept was accepted and areas of improvement for some modules were identified.

VIII. CONCLUSIONS

The aim of this paper was to describe a methodology to build and validate ATM security prototypes. This was implemented by combining well-known methodologies like SecRAM and E-OCVM. The result can be used as a blueprint for successful security prototype validation. This approach was exemplified using a dedicated prototype. The conclusions can be divided into prototype-specific results and the practicability of the elaborated methodological approach.

Regarding the prototype results it has to be kept in mind that for SACom it is very hard to clearly separate and distinguish security events from safety events based on software algorithms solely. Aircraft (hence pilots) deviating from a given ATC clearance may do this because of safety reasons (e.g. loss of control) and/or security reasons (e.g. hijacking). Detection systems like the SACom can hardly distinguish between both with only one indicator (e.g. aircraft deviations). Only a correlation of several indicators can identify a security incident [26]. As a fundamental finding a system like SACom will be useful for safety purposes, too. During validation, the SACom prototype clearly showed potential as an assistance system for handling the simulated events, especially the conformance monitoring function and the enhanced conflict detection function. Both functions need continuous, correct, complete and reliable updates about given ATC clearances, which underlines again the potential of the combination of such tools with speech recognition.

Concerning the practicability of the elaborated methodology, this approach seems to be straightforward and promising. The achieved results foster the idea to postulate a comprehensive methodology for validating ATM security systems and ATM security prototypes. Both SecRAM and E OCVM methodologies provided practical assistance for setting up the validations. Not only the needed security control could be elaborated but also a relevant validation exercise was established.

Following the facts and methodological steps a blueprint for validation of ATM security prototypes looks as follows:

- Identify the problem, PA, SA, threats and vulnerabilities.
- Gather PA, SA and analyze risk by applying SecRAM.
- Identify relevant KPI and prototype requirements.
- Build up the prototype.
- Postulate validation objectives.
- Invent scenarios for validation.
- Evaluate the prototype according to E-OCVM.

The comprehensive approach for validation of air traffic management security prototypes has been conducted the first time within the ATM security research by the project GAMMA.

ACKNOWLEDGMENT

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

REFERENCES

[1] ICAO, “Safety Management,” Annex 19 to the Convention on International Civil Aviation, 1st Edition, 2013.

[2] CSFI ATC Cyber Security Project, www.csfi.us, July 2015.

[3] EU_ECAC CASE project, https://www.ecac-ceac.org/ec-ecac-case-project.

[4] GAMMA Consortium, 2015, GAMMA CONOPS, Rev. 01.00, http://www.gamma-project.eu/wp-content/uploads/2013/11/GAMMA-Concept-of-Operations_Rev-01-00.pdf.

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

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

[7] Kreuz, M., "Modellierung von Flugsicherungsprozessen auf Basis von System Dynamics," Forschungsbericht/DLR, Deutsches Zentrum für Luft- und Raumfahrt, 2015, 33.

[8] Kölle, R., Proceedings International Summer School on Aviation Psychology (ISAP), Graz July 2007.

[9] P. Montefusco, R. Casar, R. Koelle, T. H. Stelkens-Kobsch, "Addressing security in the ATM environment: from identification to validation of security countermeasures with introduction of new security capabilities in the ATM system context," ARES, 2016 11th, 532-541.

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

[11] GAMMA consortium, 2015, D2.2 – Security objective report.

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

[13] GAMMA consortium, 2015, D2.3 – Risk treatment report.

[14] P. Montefusco, "GAMMA Security Risk Assessment and Treatment," presentation for advisory board of GAMMA, Brussels, December 2015.

[15] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, C. Neeteson, „Towards a more secure ATC voice communications system," Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th, DOI: 10.1109/DASC.2015.7311419.

[16] M. Strohmeier, M. Schaefer, R. Pinheitro, V. Lenders, I. Martinovic, "On Perception and Reality in Wireless Air Traffic Communications Security," arXiv preprint arXiv:1602.08777, DOI: 10.1109/TITS.2016.2612584.

[17] LiveATC, "Fake ATC in Action (LTBA – Istanbul)", May 2011, http://www.liveatc.net/forums/atcaviation-audio-clips/25-may-2011-fake-atc-in-action-%28ltba-istanbul%29.

[18] The Age, "Lone-wolf radio hoaxer hacks Melbourne air traffic control", November 2016, http://www.theage.com.au/victoria/lonewolf-radio-hoaxer-hacks-melbourne-air-traffic-control-afp-20161107-gsk12o.html.

[19] ICAO, "Procedures for Air Navigation Services - Air Traffic Management," Doc 4444, 15th Edition, 2007.

[20] ICAO, "Communication Systems," Annex 10 to the Convention on International Civil Aviation Vol. III, 2nd Edition, 2001.

[21] C. Neeteson, M. Rusko, "WP6 Secure ATC Communication (SACom)," presentation at GAMMA WP6 kick off meeting, Rome, February 2015.

[22] GAMMA consortium, 2015, D5.1 – Validation exercise plan.

[23] T. H. Stelkens-Kobsch, M. Finke, D. Kolev, R. Koelle, R. Lahaije, „Towards validating a security situation management capability," Integrated Communications Navigation and Surveillance (ICNS), 2016, 1A1-1-1A1-9, DOI: 10.1109/ICNSURV.2016.7486320.

[24] Helmke, H., Rataj, J., Mühlhausen, T., Ohneiser, O., H. Ehr, H., Kleinert, M., Oualil, Y, Schulder, M. and Klakow, D., "Assistant-based speech recognition for ATM applications," 11th FAA/EUROCONTROL ATM-seminar, Lissabon, Portugal, June 2015.

[25] H. Helmke, O. Ohneiser, T. Mühlhausen, M. Wies, "Reducing Controller Workload with Automatic Speech Recognition", 35th Digital Avionics System Conference, Sacramento, CA, USA, September 2016.

[26] T. H. Stelkens-Kobsch, M. Finke, M Kleinert, M. Schaper, „Validating an ATM security prototype – first results," DASC, 2016 IEEE/AIAA 35th, DOI: 10.1109/DASC.2016.7778107.

EMAIL ADDRESSES

Tim.Stelkens-Kobsch@dlr.de

Michael.Finke@dlr.de

Nils.Carstengerdes@dlr.de

The research leading to the results presented in this paper has received funding from the European Union FP7 under grant agreement no 312382. More information can be found under www.gamma-project.eu.

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)*

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 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.

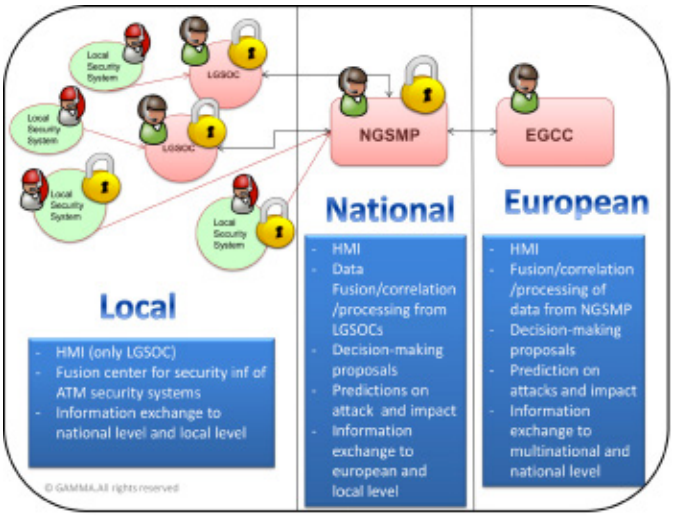


Figure 1: Overall GAMMA solution [9]

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).

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

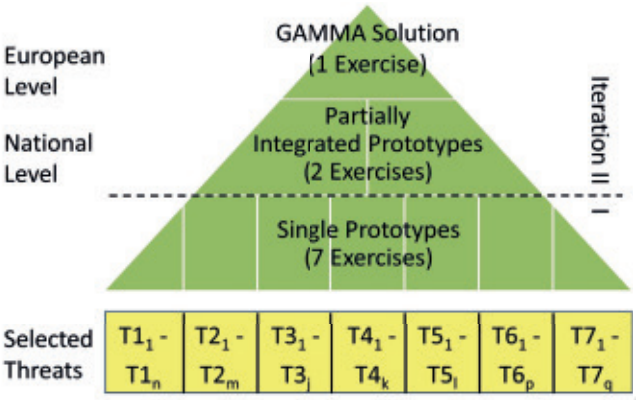


Figure 2: Validation activities overview

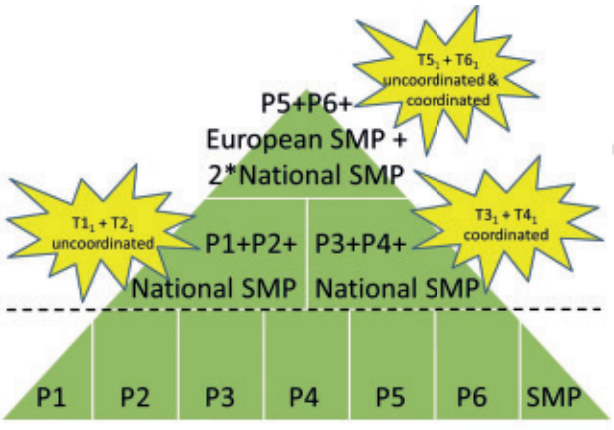


Figure 3: Selected threates and prototypes for second validation iteration.

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

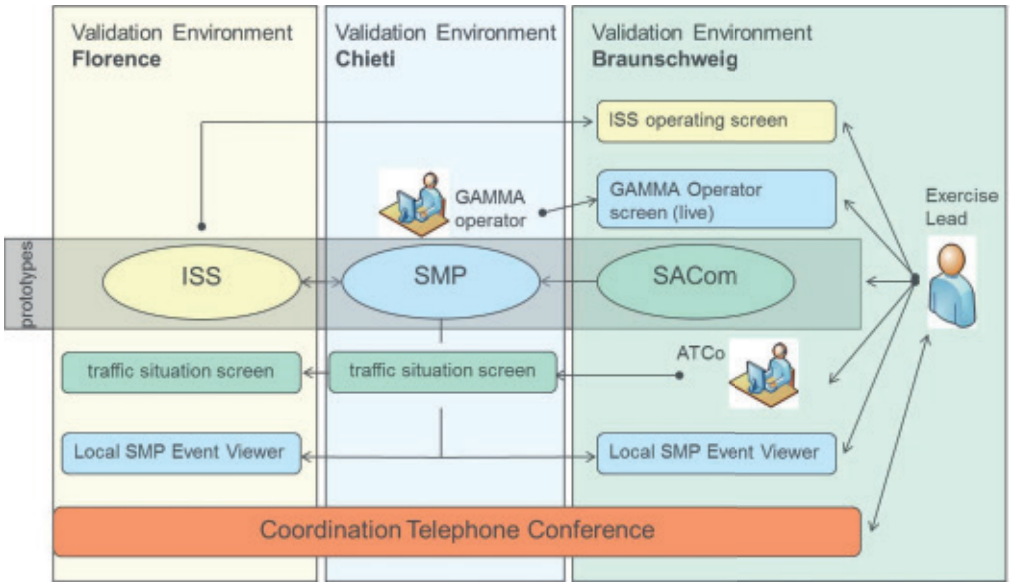


Figure 4: Schematic representation of the geo-distributed validation setup; arrows indicate the data flow.

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 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.

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.

Figure 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.

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

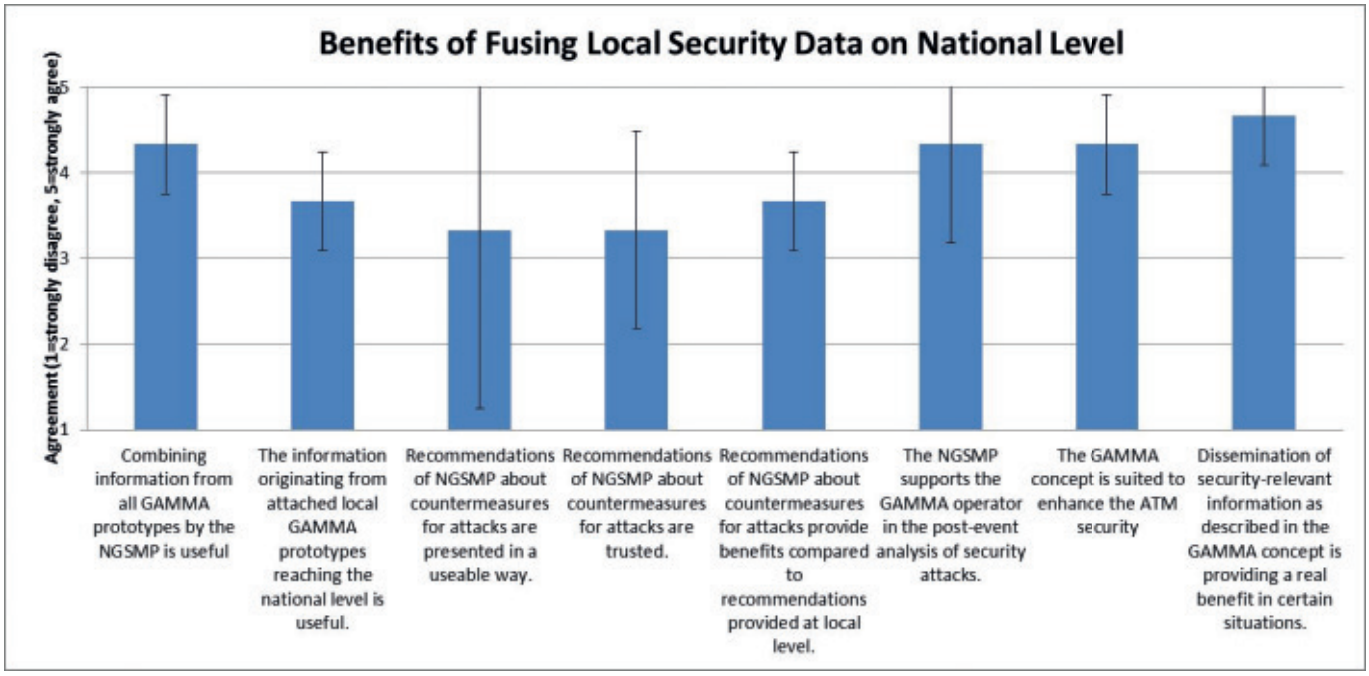


Figure 6: Benefits of fusing local security data on national level

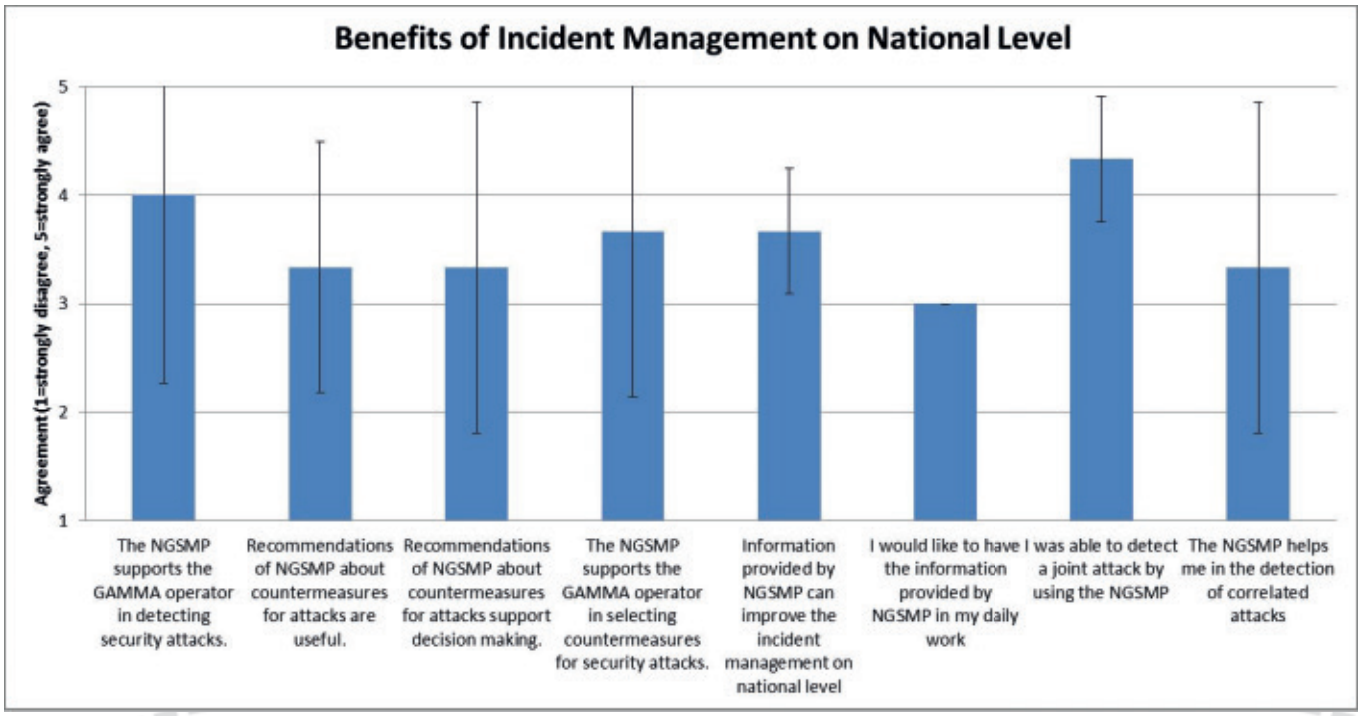


Figure 7: Benefits of incident management on national level

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 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.

EMAIL ADDRESSES

Meilin.Schaper@dlr.de,

Tim.Stelkens-Kobsch@dlr.de

Nils.Carstengerdes@dlr.de

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/.

The First Performance of the Integrated GAMMA Solution: The Full 3 Validation Exercise

DLR

INTRODUCTION – RECAP OF THE GAMMA CONCEPT

After three years of intense work on the ATM security risk assessment, the security management framework, the ATM security functional and operational architecture, the development of GAMMA prototypes, as well as their stand-alone validation, the project achieved good progress and demonstrated its initial capabilities. In the first half of 2017, the project was ready for the next challenge: more complex threat scenarios involving different kinds of offences targeting different weak points in the ATM system.

In addition to directly defending affected systems against the interference, the overall idea is to exchange all security-relevant information with all persons and/or entities in charge, also involving civil-military cooperation. This significantly improves the overall awareness of any cyber attacks and the consequences, which enable to select countermeasures more appropriately, initiate coordinated countermeasures or activate preventive measures in advance.

The GAMMA solution has come up with a multi-level approach:

- ATM Security Management on Local Level: Security Management within an ATC unit, at an airport, at an aeronautical information management unit, at a unit of the weather service, within an airplane
- ATM Security Management on National Level: Information are collected and decisions are made for all units and stakeholders within a country
- ATM Security Management on European Level: Information are collected and decisions are made for all lower GAMMA levels within Europe

Six of seven prototypes developed within GAMMA are specific security systems designed for the local level: Information Exchange Gateway (IEG), Information Security System (ISS), Global Navigation Satellite System Security (GNSS), Secure ATC Communications (SACom), Satellite Communications Security (SATCOM) and Integrated Modular Communication Security (IMC) prototypes. All these systems work as detectors and collect information about ongoing attacks on systems where they have been installed. Some prototypes are even able to directly protect those installations and/or provide assistance to the user on local level in handling the incident.

The seventh prototype is the 'core' of the whole ATM security management solution of GAMMA: the so called Security Management Platform (SMP) which collects all security relevant information generated at the local level, builds up a complete security picture, detects coherencies by correlation algorithms and provides assistance in decision making for the operator who is responsible for initiating possible countermeasures. Information can be disseminated to the local level, to the higher European level or even to military authorities if deemed necessary. At this point, the GAMMA concept foresees a new role, the so called 'GAMMA operator'. This person is specialized on ATM security crisis management and well trained on relevant regulations, procedures and on technical systems playing a role in ATM.

THE THREAT – COORDINATED AND UNCOORDINATED ATTACKS

On September 11th, 2001 the world was confronted with a completely new dimension of terrorist attacks. This obviously coordinated attack was possible because of a lack of information exchange and situational awareness between security management entities although the whole attack lasted a relatively long time of more than one hour.

To be able to systematically categorize and identify coordinated attacks a clear definition is needed. For the further work in GAMMA, the following definition was found and served as a guideline:

A coordinated attack scenario is an attack, in which:

- The single attacks are of negligible effect when performed standalone due to missing synergy effects from the other single attack (e.g. distraction, overload, amplification etc.)

And/or

- The single attacks must be aimed at exactly the same target at nearly the same time.

And/or

• The single attacks must be of a similar kind and must be aimed at roughly the same sort of targets at nearly the same time.

The term 'nearly the same time' unfortunately is not that precise. Therefore, it can be further assumed that attacks happen at 'nearly the same time' when the time frames of visible effects and aftereffects overlap. This means for example if an attack takes place at timestamp T=0 and the effects and aftereffects extend up to timestamp T=20, another attack taking place at timestamp T=45 would be considered as isolated and not as happening at 'nearly the same time'.

The coordinated 9/11 attack would be a mixture of bullet point 2 and 3 above according to this definition. Two airplanes hit the World Trade Centre (WTC) in New York City, which are two single acts hitting the same target. The attack focused at the Pentagon in Washington DC used the same method: using a hijacked airplane as a weapon to cause serious damage to a building of public interest. The time frames of visible effects and aftereffects were about several days and clearly overlapped.

Within the integrated validation exercises in GAMMA different attack scenarios with a similar level of complexity were used while also several independent, uncoordinated attacks were simulated. In the Fully Integrated Validation Exercise III (or short: Full 3), a coordinated cyber-security attack on aeronautical weather information services was simulated. The goal of this coordinated attack was to manipulate safety-relevant meteorological data (namely the measured air pressure, which is essential for altimeter settings) at two different European airports in two different countries within a time interval of a few minutes. If not detected, this false information could likely cause the risk of controlled flights into terrain (CFIT), which is a well-known type of accident with a number of examples in aviation history. In parallel, an uncoordinated hacking attack to on-board communication systems from inside of an airplane was simulated.

COMBATING THE THREATS/ATTACKS

On local level, two prototypes have been developed to counteract these threats:

The IEG (Information Exchange Gateway) prototype was built by Airbus CyberSecurity to protect web services from XML-based threats like the injection of spurious weather information or different kind of attacks against the SWIM (System-wide Information Management). This prototype aims at enhancing the traditional detection approach by providing mechanisms capable of detecting offensive contents and intercepting them by applying advanced data packet inspection methods in which malicious packets are directly blocked and alerts are instantly sent to the SMP.

The second prototype on local level is the IMC prototype, which is designed to secure integrated communication networks and systems on board of an airplane and was developed by Thales UK. This prototype offers functionalities to handle on/off board application attacks, insertion of subverted software, and directly block unauthorized access to the IMC and then send report to the SMP if required.

Although the direct defense of these parts of the attack scenario was successfully accomplished on local level, there is still no awareness about the magnitude, the potential and the coordinated nature of the attempts to manipulate the aeronautical weather data. This lack of awareness is very dangerous because it could well be that the coordinated attack is still ongoing and could at some time hit an unprotected system at another airport, maybe in another country. Therefore security-relevant information is shared between the different levels of the GAMMA solution (see Figure 1). The IEG prototypes that defended the attempts send automatic reports to the national level SMP of the corresponding countries. As long as there is just one airport affected by the attack in this country, there is no possibility to already apply correlation algorithms. But as SWIM is a European-wide service, an attack on meteorological data exchanged via SWIM could be of relevance for the European level. Therefore, the GAMMA operators at national level forwards sanitized information about the attack happening in their country to the European level according to defined rules. On European level the coordinated nature of the attack is immediately detected by correlation algorithms. Several countermeasures can now be triggered, such as a general warning is distributed directly to the user via SWIM or a specific warning is sent back to national levels; either to the SMP in a third country which is not yet hit by the attack or as feedback to an already affected country giving notification that this attack is coordinated and of a bigger magnitude.

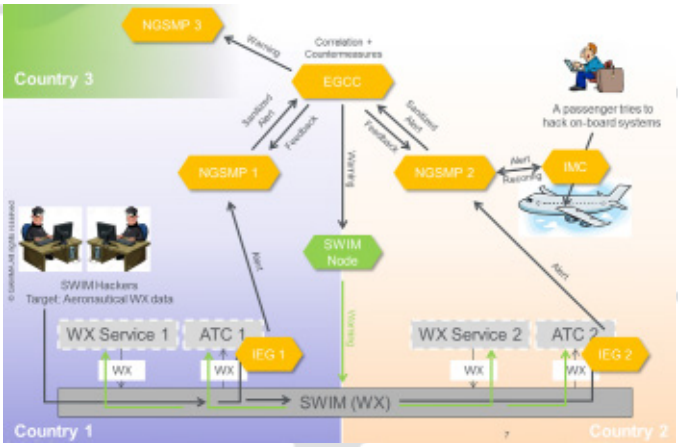


Figure 1: Attack and Response Scenario of the Full 3 Exercise

For the Full 3 exercise this scenario was successfully simulated by using a fully connected geo-distributed setup involving prototypes or system components owned by Leonardo, Airbus CyberSecurity, Thales UK,

42Solutions and Boeing Research and Technology Europe. These prototypes or system components were located in Chieti (Italy), Elancourt (France), Reading (UK), Eindhoven (Netherlands) and Madrid (Spain). Security Management Experts from the ATM domain took the role of the GAMMA operators in the final runs. The whole exercise was led by DLR using a multi-screen working position located in Braunschweig (Germany). A group of external observers from different ANSPs monitored the exercise from this position, a second group observed the exercise side-by-side with the GAMMA operators in Chieti (Italy).

The final runs of the Full 3 exercise took place on 4th May 2017 and were connected to a workshop with the mentioned experts at each site.

LESSONS LEARNED

Important outcomes of the Full III exercise were empirical data about reaction times of the GAMMA operators, transmission time of security relevant information in this geo-distributed setup and duration until the coordinated nature of the attack was identified. Additionally, it was examined if and how false alarms or missing information occur in the solution designed by GAMMA and the implications for Security Management.

In addition, valuable feedback was collected from external ATM security experts either participated as observers or as GAMMA operators, providing insights into upcoming challenges before implementing the GAMMA solution into the real world as well as benefits of the GAMMA solution provides to the ATM community as a whole; and specifically regarding ATM security improvements.

Figure 2: Multi-Screen Working Position in Braunschweig during the Final Run of the Full 3 exercise

GAMMA Consortium

Leonardo
WWW.LEONARDOCOMPANY.COM/

Airbus
WWW.AIRBUS.COM

Boeing
WWW.BOEING.COM

Airbus Defence and Space
WWW.AIRBUS.COM

Airbus Cybersecurity
AIRBUS-CYBER-SECURITY.COM

CiaoTech
WWW.CIAOTECH.COM

DLR
WWW.DLR.DE/FL/

Airbus Group Innovations
WWW.AIRBUS.COM

ENAV
WWW.ENAV.IT

Isdefe
WWW.ISDEFE.ES

Lancaster University
WWW.LANCASTER.AC.UK

RNC Avionics
RNC-AVIONICS.COM

ROMATSA
WWW.ROMATSA.RO

SEA
WWW.SEAMILANO.EU

Thales Alenia Space
WWW.THALESALENIASPACE.COM

Thales Avionics
WWW.THALESGROUP.COM

Thales UK Research & Technology
WWW.THALESGROUP.COM/UK

Ústav Informatiky
UI.SAV.SK

42 Solutions
WWW.42SOLUTIONS.NL

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

www.gamma-project.eu

The GAMMA project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement nr. 312382