



## CONTENTS

- 1 Editorial by Giuliano D' Auria, GAMMA Project Coordinator
- 2 GAMMA Project in Brief
- 3 News
- 4 Articles: The GAMMA concept and its technical instantiation: the Security Management Platform
- 5 GAMMA Project Progress
- 6 Dissemination Activities

## EDITORIAL

In this second issue of the GAMMA newsletter, I am happy to introduce you to some important developments which have emerged from the project over the last few months, as well as the new challenges expected in 2016 as the GAMMA concept is translated into a set of prototypes and then validated in a first cycle of validation exercises.

Results emerging from GAMMA are meanwhile being reflected in the diverse dissemination activities and publications performed in the last months, that you may find listed at the end of the Newsletter. I wish to highlight, in this short introduction, the open recognition received by GAMMA during the 34th Digital Avionics Systems Conference (DASC), in which the GAMMA presenters received the 'best paper in session' award.

This newsletter opens with an article dedicated to one of the main prototypes currently being developed within the Project. The Security Management Platform (SMP) prototype represents the central instantiation of the GAMMA concept as it is the security information sharing platform which lies at the heart of the GAMMA proposal for managing ATM security in Europe.

The SMP will have a central role in the validation activities planned for GAMMA in 2016. A glimpse into how these validation exercises will be conducted is provided in the article "Roadmap for the security validation" elaborating the approach to validation adopted by GAMMA. This article will give you an inside view on the validation process and what to expect in the next few months.

In order to provide an independent assessment on the systems and how the GAMMA concept is suited to respond to the security challenges facing ATM, GAMMA intends to rely on external users and experts. I therefore take the opportunity of this newsletter to welcome users, stakeholders and security experts to engage actively with the project as it enters this crucial validation phase.

This is your chance to become engaged as an active player in the validation of GAMMA so please contact us if you are willing to come onboard!

by Giuliano D' Auria,  
GAMMA Project Coordinator

## GAMMA IN BRIEF

GRANT NUMBER:	312382
PROJECT COORDINATOR:	Finmeccanica
CONTACT PERSON:	Giuliano D'Auria giuliano.dauria@finmeccanica.com
PROJECT WEBSITE:	www.gamma-project.eu
DURATION:	48 months (from 01/09/2013)
BUDGET:	14.8 € Million

## NEWS

### GAMMA at SESAR Innovation Days 2015

The GAMMA project was present at the SESAR Innovation Days conference that was held at the start of December 2015 in Bologna. The project was successfully disseminated to a wide audience through a poster, which provided an overview of the GAMMA concept, and its validation with special focus on the Security Management Platform (SMP), which represents the core prototype specifically, created to realize the GAMMA vision. The SMP is 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.

### GAMMA represented at MILIPOL 2015 exhibition

In occasion of the Milipol'2015 exhibition, held in Paris (France) last November 2015, RNC Avionics promoted GAMMA project in general as well as the latest results reached. A number of interesting and useful comments were received from the visitors to RNC Avionics booth and new contacts made during the exhibition will be kept active for the future activities in GAMMA project.

# The GAMMA concept and its technical instantiation: the Security Management Platform

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 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:

- **Coordination and 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.

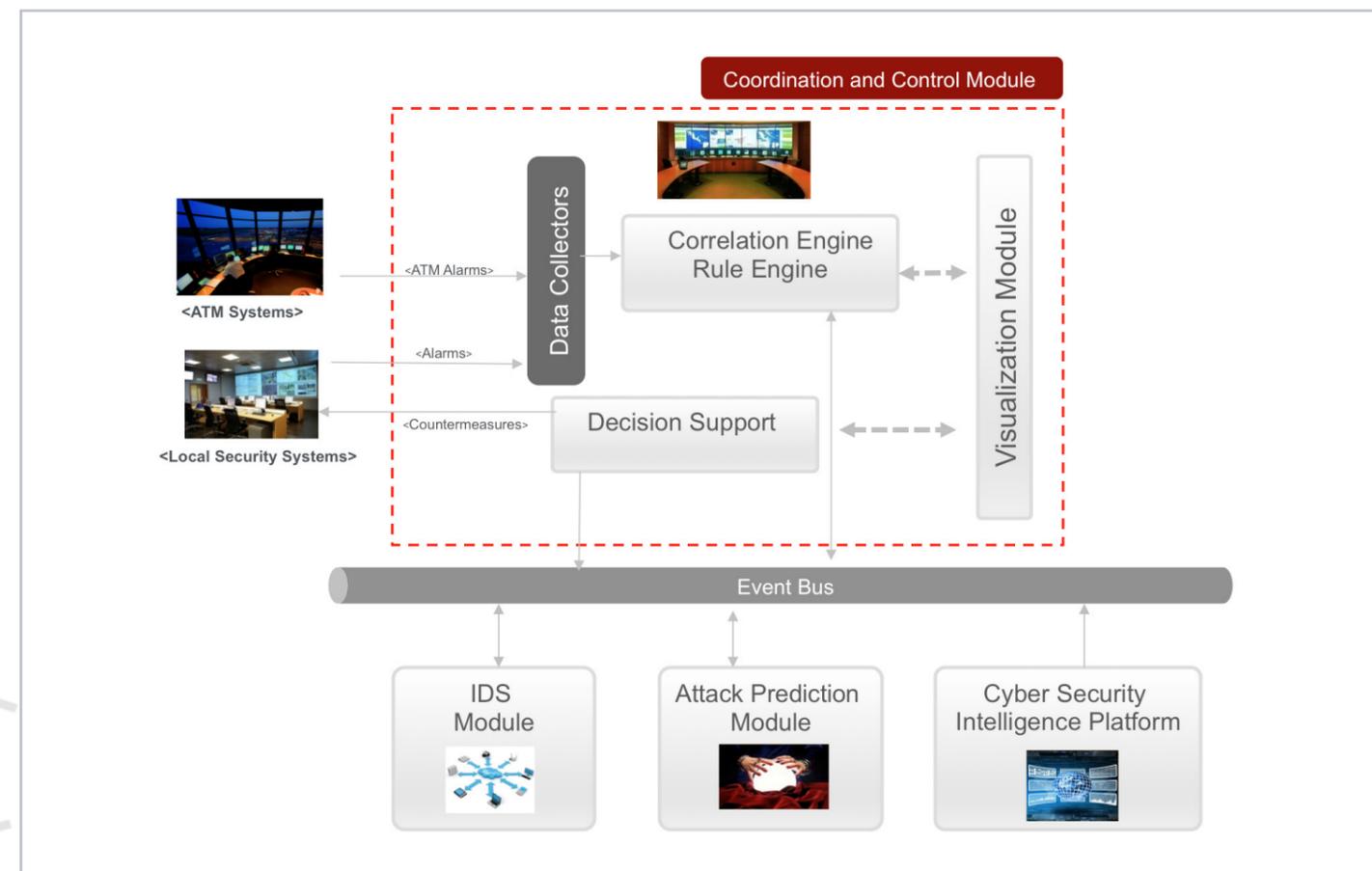
The figure represents the high level architectural layout of the Security Management Platform.

## 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 architectural lay-out

SMP 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



GAMMA PROGRESS

# Roadmap for the security validation

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.

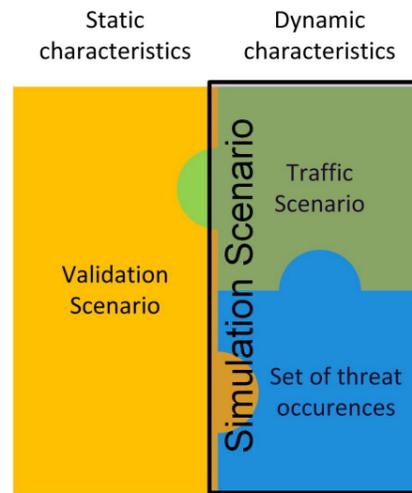


Figure 1: Illustration of the combination of a Validation Scenario, a Traffic Scenario and a set of threat occurrences as the setting for a run during a validation exercise

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.

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 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).

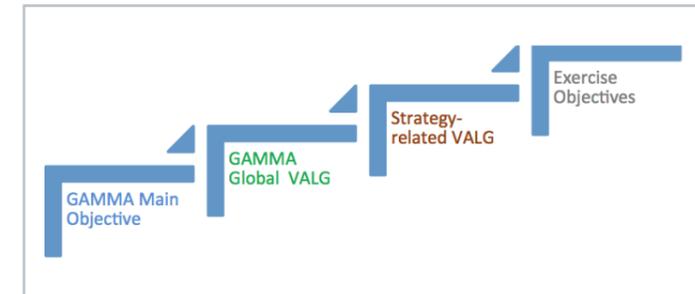


Figure 2: Validation Goals traceability path

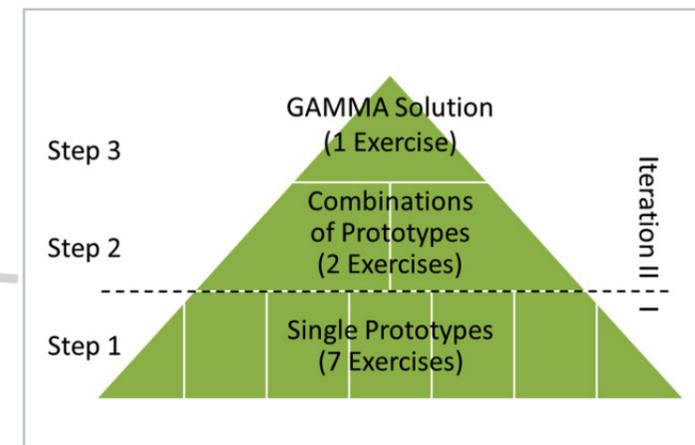


Figure 3: GAMMA validation strategy

## DISSEMINATION

### FUNDING OPPORTUNITIES

#### H2020-SESAR-2015-2 – Deadline: 16 March 2016

This is the SESAR Joint Undertakings (SJU) first main programme call for proposals - Wave 1 of its industrial research, validation and preparation for large scale demonstration activities. This call brings the results from the SESAR Programme 1, requiring further research, as well as new research content aligned with the European ATM Master Plan together in a coordinated programme of activities performed across 28 closely connected actions. This work will award as a maximum of 28 complementary grants to be awarded to the Members of the SJU and performed in the context of the SESAR2020 partnership arrangements and managed within a formal governance structure. The call is restricted to the pre-qualified 'Candidate Members' of the SJU.

#### H2020-FTIPILOT-2016 – Deadline: 25 October 2016 (cut off dates: 15 March 2016, 1 June 2016)

The FTI pilot aims to reduce the time from idea to market and to increase the participation in H2020 of industry, SMEs and first-time industry applicants. It should stimulate private sector investment, promote research and innovation with a focus on value creation, and accelerate the development of innovative products, processes and services.

#### H2020-MSCA-RISE-2016 – Deadline: 28 April 2016

The RISE scheme will promote international and inter-sector collaboration through research and innovation staff exchanges, and sharing of knowledge and ideas from research to market (and vice-versa). RISE involves organisations from the academic and non-academic sectors (in particular SMEs), based in Europe (EU Member States and Associated Countries) and outside Europe (third countries). Support is provided for the development of partnerships in the form of a joint research and innovation project. This is aimed at knowledge sharing via international as well as intersectoral mobility, based on secondments of research and innovation staff (exchanges) with an in-built return mechanism.

For more information about funding opportunities please contact [c.salas@ciaotech.com](mailto:c.salas@ciaotech.com)

### NEWS

#### GAMMA presented at the London Aerodays and Commercial UAV Show

RNC Avionics (a partner of GAMMA) presented the project and recently developed risk prediction model for ATM security management, in occasion of the AERODAYS and Commercial UAV Show, last October 2015, in London. A number of interesting discussions and new possible applications for the developed risk prediction model were discussed.

#### GAMMA presented at Le Bourget Air Show

In June 2015 GAMMA project was presented by University of Lancaster and RNC Avionics Ltd at Le Bourget Air Show in Paris where project goals and objectives, together with initial results, solutions were presented at the North West Airspace Alliance section of the UK Pavilion.

The project has gained significant interest from both the general public and ATM professionals and a number of positive comments and recommendations were received during the presentation. These suggestions will be incorporated in the ongoing research.

#### Selex ES is now Finmeccanica

From 1 January 2016, the activities of Selex ES have merged into the new Finmeccanica, operating as One Company, focusing on its core business of Aerospace, Defence and Security. The coordinator of the GAMMA project is therefore now Finmeccanica, while the working team remains the same.

### NETWORKING

#### GAMMA engaging with EASA

A GAMMA workshop with EASA is being organized in February 2016 with the aim of engaging more actively with this important stakeholder with an increasing relevance for the ATM Security domain. The workshop will provide the opportunity for GAMMA to present its activities on Security Risk assessment and Treatment, requirements definition and architecture development as well as the GAMMA concept. The meeting will then turn towards the ongoing and future activities with the aim of collecting feedback and recommendations from EASA to be considered in the future GAMMA activities.

#### GAMMA Advisory board meeting with SESAR JU

In December 2015 a GAMMA meeting was held with

SESAR JU to illustrate the work done within the project as well as ongoing and future activities. SESAR JU is a key stakeholder and part of the GAMMA Advisory Board which aims to lay out the strategic direction of the Project. The meeting in December 2015 was crucially important given the state of GAMMA which is now developing its prototypes and preparing for the validation activities. Alignment with SESAR and the SESAR 2020 preparation is of fundamental importance for the success of GAMMA.

#### GAMMA, ACARE participation and SRIA update

GAMMA partners are closely monitoring ACARE WG4 with the aim of ensuring that ideas and concepts developed in GAMMA are adequately reflected in the updated SRIA. Several GAMMA partners are involved in the new security subgroup in WG4 and following the SRIA update process. Frequent references to GAMMA in the recent workshop launching the SRIA update are evidence of the relevance of GAMMA in the definition of new security concepts for the aviation industry.

#### GAMMA engaging with other European Projects

GAMMA is building up links with other related projects with the aim of broadening the reach of technical solutions and exploring their applicability within the different domains addressed by the projects. In the last few months GAMMA has initiated coordination with the ECOSSIAN project which aims to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities. The solutions adopted by ECOSSIAN are remarkably similar to those developed by GAMMA which opens the opportunity for exchanging ideas over their implementation.

SAWSOC is another FP7 project which is being monitored by GAMMA partners in view of its activities on logical physical cross correlation of security events relating to critical infrastructure, including ATM. Especially relevant for GAMMA is the use case study conducted within SAWSOC involving the ENAV SOC (Security Operation Centre).

#### GAMMA supporting EUROCAE WG-72

GAMMA project has participated to Eurocae WG 72 contributing to a new EUROCAE directive related to aircraft and ground security items, ED 205 "Security Accreditation of ATM Systems". EUROCAE WG-72 "Aeronautical Systems Security" is

tasked to develop guidelines to address security concerns for aeronautical systems in order to ensure safe, secure and efficient operations amid the growing use of highly integrated electronic systems and network technologies used on-board aircraft.

The GAMMA project was present at the WG 72 meeting hosted by European Aviation Safety Agency (EASA) on 2 December 2015 with the aim of developing the ED-205 Statement of Work.

GAMMA expertise in the evaluation of security issues on ATM systems towards Airborne systems will support the working group by giving its ground perspective in relation to the airborne one.

#### GAMMA meets the European Defence Agency

The GAMMA Consortium has met with the European Defence Agency (EDA) and Eurocontrol with the aim of sharing a vision on the broader cyber security context in Europe. The meeting, held on 17 July 2015, served as a basis to elaborate the military perspective on the GAMMA vision and define how the military aspects should be integrated into the CONOPS. The new channel of communication opened with EDA will allow GAMMA to enrich the work performed related to the definition of the ATM Security Management System (task 3.1) with a broader military perspective.

### PUBLICATIONS

#### Paper: SECURITY SITUATION MANAGEMENT: DEVELOPING A CONCEPT OF OPERATIONS AND THREAT PREDICTION CAPABILITY

Authors: Denis Kolev, Rainer Koelle, Rosa Ana Casar Rodriguez, Patrizia Montefusco.

#### Paper: 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.

#### Paper: 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.

Documents are available for download at [www.gamma-project.eu](http://www.gamma-project.eu)

CONSORTIUM



**Finmeccanica**  
[WWW.FINMECCANICA.COM](http://WWW.FINMECCANICA.COM)



**Airbus SAS**  
[WWW.AIRBUS.COM](http://WWW.AIRBUS.COM)



**Boeing**  
[WWW.BOEING.COM](http://WWW.BOEING.COM)



**Airbus Defence and Space**  
[WWW.AIRBUSDEFENCEANDSPACE.COM](http://WWW.AIRBUSDEFENCEANDSPACE.COM)



**Airbus Defence and Space Cybersecurity**  
[WWW.CYBERSECURITY-AIRBUSDS.COM](http://WWW.CYBERSECURITY-AIRBUSDS.COM)



**CiaoTech**  
[WWW.CIAOTECH.COM](http://WWW.CIAOTECH.COM)



**DLR**  
[WWW.DLR.DE/FL/](http://WWW.DLR.DE/FL/)



**Airbus Group Innovations**  
[WWW.AIRBUSGROUP.COM](http://WWW.AIRBUSGROUP.COM)



**ENAV**  
[WWW.ENAV.IT](http://WWW.ENAV.IT)



**Isdefe**  
[WWW.ISDEFE.ES](http://WWW.ISDEFE.ES)



**Lancaster University**  
[WWW.LANCASTER.AC.UK](http://WWW.LANCASTER.AC.UK)



**RNC Avionics**  
[WWW.RNC-AVIONICS.COM](http://WWW.RNC-AVIONICS.COM)



**Romatsa**  
[WWW.ROMATSA.RO](http://WWW.ROMATSA.RO)



**SEA**  
[WWW.SEAMILANO.EU](http://WWW.SEAMILANO.EU)



**Thales Alenia Space**  
[WWW.THALESALENIASPACE.COM](http://WWW.THALESALENIASPACE.COM)



**Thales Avionics**  
[WWW.THALESGROUP.COM](http://WWW.THALESGROUP.COM)



**Thales UK Research & Technology**  
[WWW.THALESGROUP.COM/UK](http://WWW.THALESGROUP.COM/UK)



**Ustav Informatiky**  
[WWW.UI.SAV.SK](http://WWW.UI.SAV.SK)



**42 Solutions**  
[WWW.42SOLUTIONS.NL](http://WWW.42SOLUTIONS.NL)

ACKNOWLEDGEMENT



The GAMMA Project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement N° 312382.