NEWSLETTER | Issue n° 3 | September 2016

CONTENTS

EDITORIAL

I am pleased to introduce you to the third edition of the GAMMA newsletter in which we highlight some ongoing developments within the GAMMA project as well as provide a flavour of what to expect in the coming months.

This edition of the Newsletter opens with an article providing an overview of one of the prototypes which make up the GAMMA validation environment and which represents part of the overall vision proposed for the management of ATM security. The Integrated Modular Communication (IMC) prototype described in the article is an on-board platform to provide secure and reliable aircraft communications for a diverse set of applications and is viewed as an important part of the future Air Traffic Management infrastructure. Within GAMMA the security risks relevant to IMC operation have been studies and specific mitigation measures have been proposed to provide cyber resiliency for the IMC. The security controls developed as a result of this assessment will be part of the validation activities planned for the next few months.

The second main article in this Newsletter looks into the methodology adopted by GAMMA in developing the architecture representing the GAMMA proposal for managing ATM security. The choice for the framework and tool used in GAMMA has been guided by the need to remain consistent with the SESAR initiative which is using the NAF V3.1 architecture framework, and the Mega tool. The article therefore focuses on the use and tailoring of this framework within the context of the GAMMA project.

I am pleased to include within this Newsletter a short article written by the FP7 ECOSSIAN project which is aimed at improving the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures. While the scope of ECOSSIAN (covering critical infrastructures) is broader than GAMMA, the approach adopted by the two initiatives is remarkably similar as they set about defining a pan-European situational awareness framework with command and control facilities providing capabilities for the overall management of security incidents.

It is this vision which will be validated by GAMMA during the next few months and it is towards these validation actions that all eyes now turn. Please stay tuned and continue supporting us through your first hand involvement as we enter this most crucial phase for the GAMMA project!

by Giuliano d'Auria,
GAMMA Project Coordinator

GAMMA IN BRIEF

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

NEWS

Important papers have been prepared and presented by GAMMA partners in occasion of the 11th International Conference on Availability, Reliability and Security (ARES 2016) which was held at the end of August in Salzburg. Titles and authors of these papers are reported below. Documents are available for download at www.gamma-project.eu

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

Authors: Patrizia Montefusco (Traffic Control System Engineering, LEONARDO company), Rainer Koelle (School of Computing and Communications, Lancaster University), Rosana Casar (Department of Transport and Information Technology, ISDEFE), Tim H. Stelkens-Kobsch (Institute of Flight Guidance German Aerospace Center (DLR)).

Title: Security Risk Assessment and Risk Treatment for Integrated Modular Communication.

Authors: Hamid Asgari (Senior Member IEEE), Sarah Haines, and Adrian Waller.

Title: A New Vision for ATM Security Management: The Security Management Platform.

Authors: Claudio Porretti (LEONARDO company), Raoul Lahaije (42Solutions), Denis Kolev (University of Lancaster).

ARTICLES

Integrated Modular Communication in the Context of GAMMA

Author: 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.

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** applications.
Aeronautical Control & Operational communications; as a ***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; as a ***Service***	This refers to the IMC system's internal resources, configurations, and operations, e.g. processes, functions, 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** processes and the external GAMMA Security Management Platform.
Airline data; as ***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; as ***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).

Table 1: Primary Assets

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.

Supporting Asset	Description	Primary Asset
IMC system	Integrated Modular Communication 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, Airline, User, or C&M data
IMC's RaS	Converting data into a link level format, passing data to one or more transceivers	Computing resources, Airline, User, or C&M data
IMC's 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, User, or C&M data

Supporting Asset	Description	Primary Asset
Satellite link	Satellite link to provide worldwide 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 systems for on-the-ground com.	Airline, User, or C&M data
Cellular link	Provides cellular connectivity such as 3G.	User data

Table 2: Supporting Assets

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.

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 proximity to ATM channels to perform this attack. These devices prevent IMC from communicating application data.

Table 3: Identified IMC Threats

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.

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.

GAMMA Architecture Development methodology

Author: 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.

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

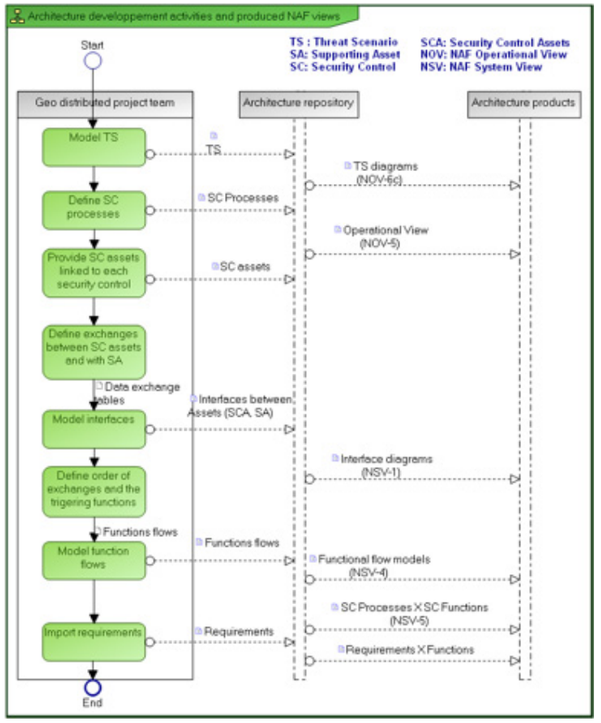


Figure 1: Architecture development activities and outcomes

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.

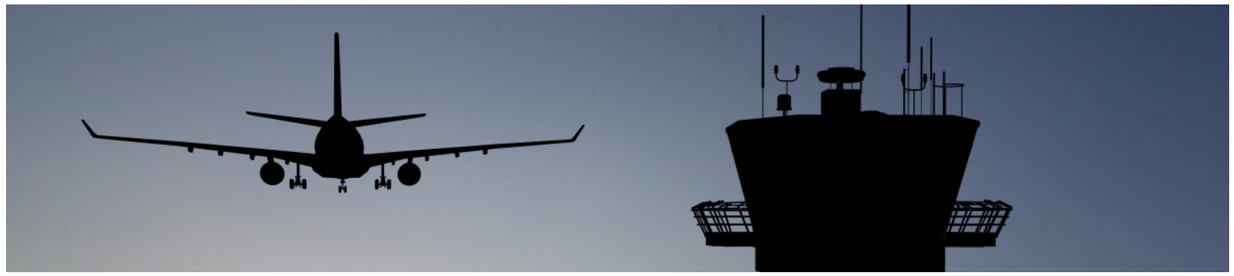
Generate models and deliverable documents

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.



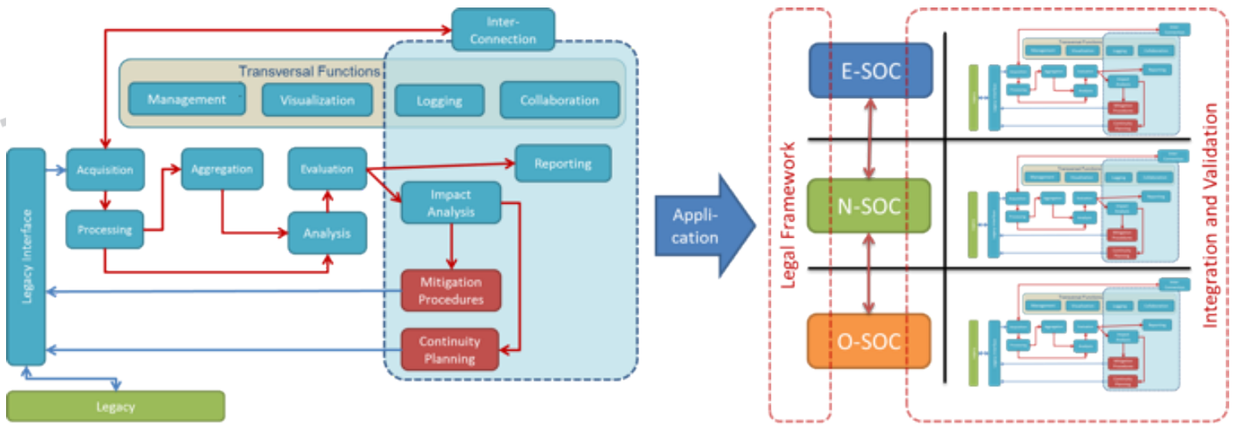
ARTICLES

ECOSSIAN technical Concept

The intention of ECOSSIAN (FP7 project, GA n° 607577) is 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.

From the technical point of view, major results came-up with the definition of the overall ECOSSIAN architecture (illustrated on the left-hand side of the drawing above) that is based on a Functional Block (FB) concept and dedicated information flows between those FBs. This overall architecture is to be instantiated and specialized for each SOC level as illustrated on the right-hand side and thus spanning the general architectural framework. Actually, functional definition of FBs and the identification of protocols and semantics of data transferred are under progress. Technical work is dedicated investigating and developing functionalities provided by the individual FBs as well as about interoperability between FBs and overall workflow. All this is in line with investigating legal conditions.

ECOSSIAN - http://ecossian.eu/



DISSEMINATION

NEWS

GAMMA presented at the 2016 EUROCAE Symposium

The GAMMA project was presented at the EUROCAE 2016 Symposium which was held in Vienna on 28 and 29 April 2016. Claudio Porretti from LEONARDO-FINMECCANICA gave a presentation focussing on the GAMMA concept and its instantiation through the Security Management Platform.
The 2016 Symposium was held in a distinctive format from previous editions, focussing not only on standardisation, but instead building the programme around five sessions in a way to convey the bigger picture of these themes: Flight Tracking, runway safety, Cyber Security, RPAS and Space Travel.
The GAMMA presentation was inserted within the dedicated session focussing on Cyber Security and stimulated considerable interest by the qualified audience. The session was followed by questions to the panel during which the GAMMA work was put into the wider context of ongoing actions on Cyber Security.

GAMMA presented at NEASCOG Cyber Security Seminar

A presentation on the GAMMA Security Management Platform was given by Claudio Porretti from LEONARDO-FINMECCANICA at the Cyber Security Seminar organised by the NATO/EUROCONTROL ATM Security Coordinating Group (NEASCOG) on 9 and 10 June 2016.
The seminar was intended to provide an overview of current activities, future plans and main concerns across aviation stakeholders and other organisations dealing with cyber security. A large audience of NEASCOG members and other aviation stakeholders dealing with Cyber Security attended the seminar.
The GAMMA presentation, which mainly focused on the SMP functionalities and modules, highlighted the central role played by the Security Management Platform (SMP) within the GAMMA concept. In the discussion following the presentation the communalities between the GAMMA Concept and the Centralized Services promoted by EUROCONTROL where highlighted by various participants.
GAMMA has become a regular contributor to NEASCOG events and in a similar conference organized in June 2015 GAMMA was present with a stand exhibiting the results and achievements from the project.

GAMMA at ART Workshop on ATM Security and Cybersecurity

On 23rd March 2016, GAMMA participated to the Workshop on ATM Security and Cybersecurity organised by the EUROCONTROL Agency Research Team (ART).
ART advises EUROCONTROL on all aspects related to research and development and represents external stakeholders from ANSP, academia and research centres, SMEs and industry.
The ATM Security and Cybersecurity Workshop was part of ART's programme devoted to selected topics of great and growing importance for ATM.
The workshop was the opportunity for GAMMA to present latest developments in the Project with a presentation focusing on the GAMMA concept and its instantiation through the SMP prototype. The meeting proved an excellent opportunity to meet stakeholders with an interest in GAMMA and in the forthcoming validation activities.

GAMMA demo presented to the Dutch Ministry of Defence

During the NIDV regional day, Eindhoven on April 15th 2016, the new Director of the Defence Materiel Organisation (DMO) got acquainted with NIDV SME members (link). During this day, 42 Solutions (partner of GAMMA) gave a demonstration to DMO of the Dutch Ministry of Defence of the capabilities of the GAMMA Security Management Platform IDS module. This demo shows a scenario of a RPAS threat near airport Schiphol in the Netherlands where Dutch military police and national police report to LNVL on the progress of dealing with the RPAS threat.

Colloquium on ATM security at DLR

On the 25th and 26th of August 2016, DLR (a partner in GAMMA Project) organised a colloquium on ATM security, aiming to discuss and identify various current and potential security threats to ATM. GAMMA project was well represented at this event with presentations from THALES UK Limited and Lancaster University. Both presentations were accepted with great interest with numerous follow up questions and discussions.

NETWORKING

GAMMA takes part in the ECOSSIAN Project meeting with Advisory Board

On the 12th of May, GAMMA joined the ECOSSIAN FP7 project in a dedicated meeting with their Advisory board. GAMMA and ECOSSIAN have joined forces in the recognition that both projects have come up with remarkably similar proposals for tacking the challenges of security at a European Level. While the objective of GAMMA is to develop security solutions relating to the ATM domain, the intention of ECOSSIAN is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures. Both projects foresee multilayer solutions based on implementing a pan-European early warning and situational awareness framework. The two projects have already exchanged relevant information and GAMMA intends to involve key ECOSSIAN partners in the forthcoming validation activities. The meeting held in Dublin was an excellent opportunity to discuss and review the work done within ECOSSIAN and gather lessons applicable within the frame of the GAMMA activities.

FUNDING OPPORTUNITIES

H2020-SESAR-2016-1– Deadline: 25 October 2016

As part of SESAR 2020, the SESAR Joint Undertaking is seeking through this call to stimulate innovative players to explore initial solutions for a new unmanned traffic management ("UTM") system supporting the cohabitation/sharing of airspace of manned and unmanned systems, which represents a critical market enabler that has not yet been sufficiently addressed at the European level. The SESAR Exploratory Research into Remotely Piloted Aircraft Systems (RPAS) and Unmanned Aircraft Systems (UAS) will address the key research questions impacting the operation of UAS and RPAS in the very low level (VLL), including beyond visual line of sight (B-VLOS) operations, as well as visual flight rules (VFR) environments (noting that the topic of instrument flight rules (IFR) integration will be addressed in other components of the SESAR 2020 Programme). Two work areas are defined under this call; these are UAS/RPAS integration operational issues and UAS/RPAS integration technical issues. The first work area on UAS/RPAS integration operational issues (Work Area 1) includes one topic while Work Area 2 is split into 6 further topics.

H2020-FTIPILOT-2016 – Deadline: 25 October 2016

The FTI pilot aims to reduce the time from idea to market and to increase the participation in Horizon 2020 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-CS2-CFP04-2016-02 - Deadline 5 October 2016

By spearheading European aeronautics research culminating in demonstrations of game-changing new vehicle configurations, Clean Sky 2 will enable the aeronautics industry to introduce innovations in timescales that would otherwise be unachievable. The 4th Call for Proposals is now published and it includes 57 topics covering the following areas: Large Passenger Aircraft IAPD, Regional Aircraft IADP, Fast Rotorcraft IADP, Airframe ITD, Engines ITD, and Systems ITD.

SMEInst-10-2016-2017: Small business innovation research for Transport and Smart Cities Mobility– Deadlines Phase 1 in 2016: 9 November 2016 - Deadlines Phase 2 in 2016: 13 October 2016

The SME instrument addresses the financing needs of internationally oriented SMEs, in implementing high-risk and high-potential innovation ideas. It aims at supporting projects with a European dimension that lead to major changes in how business (product, processes, services, marketing etc.) is done. Actions to develop new services, products, processes, technologies, systems and combinations thereof that contribute to achieving the European transport and mobility goals defined in the 2011 Transport White Paper could be particularly suited for this call.

H2020-MSCA-RISE-2017 – Deadline: 5 April 2017

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.

H2020-MG-1.2-2017 Reducing Aviation noise – Deadline: 26 January 2017 (first stage)

Despite significant progress on noise reduction at source and on noise abatement procedures, aircraft noise continues to cause adverse effects on quality of life and on public health. Actions should address the development of new technologies and methodologies to enable 24/7 operations, including new methods for assessing, monitoring and managing the impact of aviation noise. They should also support the coordination of national and EU research activities related to aviation noise and consider possibilities for international cooperation.

H2020-MG-1.3-2017 - Maintaining industrial leadership in aeronautics – Deadline: 26 January 2017 (first stage)

European aeronautics has never been stronger, however new opportunities and challenges lie towards 2020 and beyond. Research and innovation is the main response towards maintaining the competitiveness throughout the whole supply chain. Primes, suppliers including SMEs, research laboratories and academia should collaborate in an efficient and timely manner to bring innovative technologies to higher maturity levels for these advanced and cost-efficient products and services.

H2020-MG-1.4-2016-2017 - Breakthrough innovation - Deadline: 26 January 2017 (first stage)

The aim is to develop exploitable breakthrough technologies and concepts for the medium term that are not currently used or that have not yet being put in combination for civil aviation. The actions should target technologies and concepts that are at low Technology Readiness Level today (up to TRL 3) and can potentially achieve Technology Readiness Level 6 by 2030-2035. The actions should focus to airframe, propulsion and on-board systems & equipment, including their integration and may challenge established practices.

H2020-MG-1.5-2016-2017 - Identification of gaps, barriers and needs in the aviation research - Deadline: 26 January 2017 (first stage)

In 2017, the actions should provide on an annual basis a review of the state of the art of research and innovation including international benchmarking, identify gaps in the research landscape, bottlenecks to innovation (regulation, financing) and formulate recommendations to address those. The actions should address one or several of the following research domains of the ACARE Strategic Research and Innovation Agenda: Mobility, Competitiveness, Environment and energy, Safety and security.

H2020-GALILEO-1-2017 EGNSS Transport applications – Deadline: 1 March 2017

Proposals should aim at developing new innovative applications, with commercial impact and a clear market uptake perspective. The specific challenge of this topic is to develop innovative EGNSS based applications in aviation, road, maritime and rail that will make EGNOS and Galileo more available to transport users and enable new end-to-end solutions that require accurate and resilient positioning and navigation.

For more information about funding opportunities please contact c.salas@ciaotech.com.

CONSORTIUM

LEONARDO
WWW.LEONARDOCOMPANY.COM

Airbus SAS
WWW.AIRBUS.COM

Boeing
WWW.BOEING.COM

Airbus Defence and Space
WWW.AIRBUSDEFENCEANDSPACE.COM

Airbus Defence and Space Cybersecurity
WWW.CYBERSECURITY-AIRBUSDS.COM

CiaoTech
WWW.CIAOTECH.COM

DLR
WWW.DLR.DE/FL/

Airbus Group Innovations
WWW.AIRBUSGROUP.COM

ENAV
WWW.ENAV.IT

Isdefe
WWW.ISDEFE.ES

Lancaster University
WWW.LANCASTER.AC.UK

RNC Avionics
WWW.RNC-AVIONICS.COM

Romatsa
WWW.ROMATSA.RO

SEA
WWW.SEAMILANO.EU

Thales Alenia Space
WWW.THALESALENIASPACE..COM

Thales Avionics
WWW.THALESGROUP.COM

Thales UK Limited
WWW.THALESGROUP.COM/UK

Ústav Informatiky
UI.SAV.SK

42 Solutions
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.